MITIGAR LOS RIESGOS DE ATAQUES A BASES DE DATOS POSTGRESQL, DE LA FAMILIA DE LAS VERSIONES 9.X, EN AMBIENTES WEB.

JOSÉ ALAIN SALAZAR CATAÑO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍAS E INGENIERÍAS

Cartago

2020

MITIGAR LOS RIESGOS DE ATAQUES A BASES DE DATOS POSTGRESQL, DE LA FAMILIA DE LAS VERSIONES 9.X, EN AMBIENTES WEB.

JOSÉ ALAIN SALAZAR CATAÑO

MONOGRAFÍA

FREY DE JESÚS CASTRO RAMÍREZ
Director del Proyecto

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍAS E INGENIERÍAS

Cartago

2020

Nota de Aceptación

_____
_____
_____

_____
Presidente del Jurado

_____
Jurado

_____
Jurado

Dosquebradas 01 de Octubre de 2020

TABLA DE CONTENIDO

Pág.

LISTA DE TABLAS

Pág

LISTA DE FIGURAS

Pág

RESÚMEN

Postgresql pertenece a la categoría de base de datos relacionales, por esta razón es una de las opciones más interesantes, al momento de pensar en alojar y administrar la información, es utilizada para entornos cliente servidor y aplicaciones web, debido a que permite desarrollar bases de datos relacionales robustas y eficientes, sin embargo, es susceptible de ser atacada, debido a múltiples causas que generan fallas de seguridad tanto internas como externas, por esta razón es preciso referenciar que históricamente los expertos en seguridad de postgresql, han encontrado de cero a siete problemas de seguridad al año, a esto debemos añadirle que en Colombia se registran al día 542 mil ataques informáticos, donde el sector financiero es el blanco principal de estos ataques y que solo el 37% de las empresas, manifiesta estar preparado para hacer frente a un incidente digital, de este porcentaje el 70% corresponde a grandes empresas y para el caso de las microempresas solo el 45%.

Por las razones expuestas, es necesario identificar las vulnerabilidades encontradas en este manejador de base de datos, identificando las actualizaciones que corrigen dichos fallos y proponer una metodología de aseguramiento que mitigue el riesgo de intrusión que comprometa la información almacenada para las versiones de la familia 9.x de postgresql, para lograr este objetivo, es necesario realizar un análisis, que permita identificar los requerimientos de hardware y software y el tipo de implementación de seguridad, con el que debe contar un ambiente de producción de postgresql versiones 9.x en ambientes web.

ABSTRACT

Postgresql is a database management system, which belongs to the category of relational database, for this reason it is one of the most interesting options, when thinking about hosting and managing information, it is used for server client environments and web applications, because it allows the development of robust and efficient relational databases, however, it is susceptible to being attacked, due to multiple causes that generate internal and external security flaws, for this reason it is necessary to refer that the postgresql security, finds from zero to seven security problems a year, to this we must add that in Colombia there are 542 thousand computer attacks per day, where the financial sector is the main target of these attacks and only 37% of the companies, claims to be prepared to face a digital incident, of this percentage 70% corresponds to large companies and in the case of micro businesses only 45%.

For the above reasons, it is necessary to identify the vulnerabilities found in this database manager, identifying the updates that correct said failures and propose an assurance methodology that mitigates the risk of intrusion that compromises the information stored for the family versions. 9 .x postgresql, to achieve this goal, it is necessary to perform an analysis, which allows to identify the hardware and software requirements and the type of security implementation, which must have a production environment of postgresql 9.x versions in environments Web.

GLOSARIO

SGBD: (Sistema Gestor de Base de Datos), tipo de software cuya función es servir como interfaz entre la base de datos y el usuario
CVE: (Common Vulnerabilities and Exposures) Sitio encargado de recopilar y publicar las vulnerabilidades encontradas en todo tipo de software.
SSL: (Secure Sockets Layer) Es un protocolo que maneja certificados digitales, para crear comunicaciones seguras a través de internet.
NULL: Es un término utilizado en computación para referirse a nada o vacío
BÚFER: Es un tipo de memoria temporal de información, que se utiliza para transferir datos entre unidades funcionales diferentes
JSON: (Javascript Object Notation) Es un formato de intercambio de datos de notación literal que no requiere el uso de xml
CLOUDFORMS: Plataforma de gestión de infraestructura que permite al departamento de TI, gestionar máquinas virtuales, espacio en la nube, entre otros.
CRYPTOVIRUS: Es un tipo de troyano que encripta la información y la deja inaccesible para su dueño, este tipo de ataque se llama ransomware
PENT TEST: Pruebas de penetración para poner a prueba un sistema informático, red o aplicativo web, en busca de vulnerabilidades.
SNIFFER: Programa para redes que permite capturar paquetes que viajan por una red.
BACKDOOR: Programa diseñado para abrir una puerta trasera en un sistema, de tal forma que le permita al diseñador del backdoor tener acceso al sistema.
ROOTKITS: Es un conjunto de herramientas que le permiten a un atacante que ha accedido a un sistema, esconder procesos y archivos para mantener el acceso.
CORE: Palabra en ingles que significa núcleo.
RELEASE: En informática se utiliza para denotar versión
CLUSTER: Arquitectura que provee una colección de componentes, que se unen para proveer alta disponibilidad.
SMTP: Es un protocolo para la transferencia simple de correo, que se utiliza para el intercambio de correo electrónico.
CROSS-SITE-SCRIPTING: Es un tipo de vulnerabilidad típico de aplicaciones web, que puede ser usado para que un atacante introduzca código javascript.
ASCCI: Es un Sistema de codificación por el cual las letras números y caracteres se les asigna un número del 0 al 127 a cada número, letra o carácter especial.
FRAMEWORK: Es un entorno de trabajo o conjunto estandarizado, que sirve para la organización y desarrollo de software.
OWASP: (Open Web Application Security Proyect) Es un proyecto de código abierto dedicado a combatir y determinar las causas que hacen que el software sea inseguro.
REST: Es una interfaz que usa HTTP para tratar datos que provienen de formatos como JSON Y XML
SOAP: Es un protocolo que define como dos objetos de diferentes procesos, pueden comunicarse por medio de XML

HARDENING: Es el proceso de asegurar un sistema, utilizando la reducción de vulnerabilidades, el cual se logra eliminando usuarios, software y servicios innecesarios y cerrando puertos que no se utilicen.

INTRODUCCIÓN

Producto de la globalización, las organizaciones utilizan plataformas digitales que le permiten al cliente final, acceder a todos los productos y/o servicios ofertados por esta, si bien es cierto internet les ofrece la posibilidad de acceder a cada rincón de la tierra, sin tener una persona físicamente en cada localidad o municipio del planeta ya que a un simple clic, el cliente descubre un mundo lleno de oportunidades y opciones disponibles para su consumo, sin embargo existe el temor de no utilizar dichos servicios, por miedo a que sus datos personales y financieros sean revelados, lo que supondría enormes fugas de información no solo financieras sino también de datos personales, que podrían ser utilizados con fines oscuros, todo esto por falta de seguridad de la plataforma digital, ofrecida por las organizaciones que la utilizan para competir en el ámbito nacional e internacional, por este motivo alojar y almacenar información, puede convertirse en un dolor de cabeza, si no se cuenta con las medidas necesarias en cuanto a configuración y protección de la base de datos, ya que los atacantes se encuentran a la espera de encontrar un sistema que no haya sido configurado correctamente o con un sistema de seguridad débil, que les permita tener acceso a la información, explotando las diferentes vulnerabilidades encontradas a nivel de sistema operativo, red de datos, aplicación y manejador de base de datos.

Por tanto, proteger y preservar las propiedades de la información (Integridad, Confidencialidad y Disponibilidad), debe ser el objetivo principal de las soluciones informáticas implementadas por cada organización, valiéndose del uso de herramientas especializadas, que permiten el escaneo de vulnerabilidades y fallas de seguridad para que mediante un ciclo de mejora continuo, vislumbre aquellas debilidades y oportunidades de mejora, que conlleve al fortalecimiento de las plataformas tecnológicas para que cumplan con la finalidad de asegurar el patrimonio más valioso de las organizaciones, la información.

Pero esta tarea, a cargo del profesional de la seguridad informática debe ir de la mano con el (DBA) administrador de la base de datos, ya que en la mayoría de los casos, esta tarea se encuentra dividida y cada uno actúa por su lado tratando de asegurar lo que le corresponde, así que el trabajo armónico entre estas dos personas, es el camino para que una infraestructura de seguridad funcione y cumpla con el objetivo de estar un paso adelante para mitigar los riegos de intrusión y pérdida de información.

El presente trabajo tiene como objeto, consultar y analizar las diferentes fuentes de información, que documentan las vulnerabilidades encontradas en el manejador de base de datos PostgreSQL, en las versiones 9.x, los patrones utilizados para realizar ataques en ambientes web, describir la anatomía de un ataque informático, identificar las actualizaciones de seguridad publicadas por el

fabricante PostgreSql que corrigen fallos de seguridad, consultar la normatividad vigente en el país acerca de los delitos informáticos y determinar la importancia de realizar una adecuada configuración inicial de la base de datos, realizando un endurecimiento de la misma, con el fin de construir y proponer una serie de procedimientos, que mitiguen los riesgos de intrusión en un ambiente de producción, ofreciendo a las organizaciones, elementos de juicio que los ayude a crear un ambiente de confianza y fortaleza en la seguridad de la información.

1. PLANTEAMIENTO DEL PROBLEMA

En la actualidad Postgresql sufre ataques de inyección SQL, elevación de privilegios, malware, uso excesivo de privilegios y denegación del servicio a causa del mal diseño de las aplicaciones, bases de datos mal configuradas, falta de actualizaciones tanto del sistema operativo como del sistema gestor de base de datos, redes y sistemas operativos expuestos, por falta de hardware y/o software que impida o detecte el acceso no autorizado a las redes locales y al equipo que alberga el sistema gestor de la base de datos postgresql.

Según un informe de TECNONUCLEOUS El ataque más conocido a postgresql se presentó mediante malware donde se utilizó una imagen de la actriz scarlett Johansson, que contenía una carga maliciosa para luego instalarse como un minero de monero, este ataque fue descubierto por el honeypot de la firma de seguridad imperva, revelando que más de 710,000 servidores estaban visibles en internet y eran vulnerables a este tipo de ataque.

Así mismo durante el primer trimestre de 2018 el common vulnerabilities and exposures (CVE), reveló 4 vulnerabilidades encontradas en el SGBD que permitía que un atacante autenticado leyera bytes de la memoria del servidor, leer o modificar archivos que pueden contener contraseñas de base de datos cifradas y no cifradas, escalar privilegios y ejecutar código con permiso de superusuario en la base de datos. [1]

Ante este panorama es necesario que las organizaciones, independiente de su tamaño, cuenten con una política de seguridad, preferiblemente basada en prevención que cumpla con los criterios de configuración, cambio constante de contraseñas, software de monitoreo, programas de auditoria y aplicación de parches. [2]
Por lo expuesto anteriormente, surge el siguiente planteamiento del problema:
¿Cómo Mitigar los riesgos de ataques a bases de datos postgresql, de la familia de las versiones 9.x, en ambientes web.?

[1] SEVERAL NINES. Principales amenazas de seguridad de Postgresql, [En línea]. Disponible en: https://severalnines.com/database-blog/top-postgresql-security-threats [Accedido Noviembre 2019]
[2] VILLALOBOS Johnny. Vulnerabilidades de Sistemas Gestores de Base de Datos, [En línea]. Disponible en:
https://www.redalyc.org/html/4759/475948929016/
[Accedido Noviembre 2018]

2. JUSTIFICACIÓN

Las organizaciones, buscan competir en el ámbito nacional e internacional, haciendo visible sus productos y servicios y que mejor que la red de redes (internet), es así como diseñan grandes plataformas web donde publicitan y realizan una gran cantidad de transacciones, ofreciendo al cliente para que, desde la comodidad de su hogar, puede hacerse de los servicios ofertados.

Contar con toda esta información, ha cambiado la forma de hacer comercio, ya no se puede esperar a que el cliente venga buscando productos o servicios, ya se cuenta con todo un sistema que perfila e inclusive predice los hábitos de consumo de las personas.

Estos grandes volúmenes de información, deben almacenarse en bases de datos que permitan su administración y análisis, es allí cuando los sistemas de gestión de bases de datos como postgresql, aparecen con sus grandes fortalezas para ofrecer soluciones robustas y eficientes, sin embargo aunque la seguridad de la información, siempre está amenazada, debido a los ataques mencionados, es necesario plantear una metodología que contemple las vulnerabilidades a la cual se encuentra expuesta el motor de base de datos y los procedimientos que ayudarán a mitigar el riesgo de sufrir un ataque que comprometa la integridad, confiabilidad y disponibilidad de la información, esta solución permitirá al profesional en seguridad informática, realizar las configuraciones de cambio de contraseñas por defecto de la instalación inicial, para prevenir ataques por base de datos no configuradas, configurar privilegios estrictamente necesarios y definir los permisos de acceso a la base de datos para cada cuenta para prevenir ataques por uso excesivo de privilegios, aplicar las actualizaciones publicadas por el fabricante para prevenir ataques de inyección SQL, usar tecnologías WAF, para prevenir tráfico malicioso, crear un esquema de seguridad a nivel de usuario y sistema operativo utilizando antivirus basados en tecnología EDR (Endpoint Detection and Response) para prevenir ataques por malware y finalmente la utilización de suites como OWASP y KALI Linux, que permiten realizar pruebas de intrusión para buscar vulnerabilidades y así prevenir ataques por intrusiones a la base de datos PostgreSQL.

Para esto se detalla en qué consisten estos ataques, como mitigar cada uno de ellos y como realizar configuraciones a nivel de base de datos y aplicación, para evitar entradas no permitidas de información que terminen en ataques de inyección SQL, desbordamiento de búfer, denegación de servicio, configuraciones por defecto, malware entre otros.

3. OBJETIVOS

3.1 GENERAL

Determinar las vulnerabilidades existentes en las bases de datos postgresql, versiones 9x, con el fin de mitigar los riesgos y reducir la posibilidad de intrusión en un 70%.

3.2 ESPECÍFICOS

- Describir las vulnerabilidades encontradas a la familia de las versiones 9.x, las cuales han sido reportadas al CVE (Common Vulnerabilities and Exposures).

- Identificar las actualizaciones que corrigen las vulnerabilidades que afectan la familia de las versiones 9.x

- Documentar los procedimientos establecidos para prevenir, ataques por fallas o vulnerabilidades del sistema de gestión de base de datos.

- Proponer una metodología de aseguramiento que mitigue el riesgo de intrusión, para la familia de versiones postgresql 9.x.

4. MARCO TEÓRICO

4.1 MARCO DE REFERENCIA

Dentro de este marco es necesario documentar las principales vulnerabilidades encontradas, a las versiones de la familia 9.x de PostgreSQL reportadas al CVE y Aspectos a tener en cuenta para la seguridad de la base de datos PostgreSQL

4.1.1 Reporte de Vulnerabilidades de PostgreSQL Familia 9.x

- CVE-2015-3165: Vulnerabilidad que permite al atacante remoto efectuar bloqueo o denegación del servicio cerrando una sesión SSL, en el tiempo de espera de autenticación. [3]

- CVE-2015-3427: Vulnerabilidad que permite a los atacantes remotos, ataque de inyección SQL, por medio de barra invertida (\) en un mensaje. [4]

- CVE-2015-4644: Vulnerabilidad derivada de la función php_pgsql_meta_data, que no valida la extracción de token de nombre de tablas, permitiendo a los atacantes causar una denegación del servicio por la eliminación de punteros NULL. [5]

- CVE-2015-5288: Vulnerabilidad derivada de la función crypt en pgcrypto permitiendo que los atacantes puedan causar una denegación del servicio o leer la memoria del servidor. [6]

- CVE-2015-5288: Vulnerabilidad derivada de múltiples desbordamientos de búfer, en el análisis de json, permitiendo a un atacante causar una denegación del servicio, por vectores que no se manejen adecuadamente en json. [7]

- CVE-2015-7502: Vulnerabilidad derivada por las aplicaciones Management Engine (CFME) 5.4.4, CloudForms 4.0 Management Engine (CFME) 5.5.0 y Red Hat CloudForms 3.2 que no encriptan de una forma adecuada los

[3] CVE-2015-3165. Vulnerabilidad 2015-3165, [En línea]. Disponible en: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3165 . [Accedido Octubre 2018]
[4] CVE-2015-3427. Vulnerabilidad 2015-3427, [En línea]. Disponible en: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3427 . [Accedido Octubre 2018]
[5] CVE-2015-4644 Vulnerabilidad 2015-4644, [En línea]. Disponible en: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4644 . [Accedido Octubre 2018]
[6] CVE-2015-5288 Vulnerabilidad 2015-5288, [En línea]. Disponible en: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5288 . [Accedido Octubre 2018]
[7] CVE-2015-5289 Vulnerabilidad 2015-5289, [En línea]. Disponible en: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5289 . [Accedido Octubre 2018]

datos, provocando que un usuario local logre acceder a información confidencial. [8]

- CVE-2016-0766: Vulnerabilidad de PostgreSQL, que no restringe el acceso a los ajustes de configuración para PL / Java permitiendo a atacantes obtener privilegios. [9]

- CVE-2016-0767: Vulnerabilidad de PL / Java que permite a usuarios remotos autenticados con el permiso USAGE modificar el classpath del esquema público [10]

- CVE-2016-0768: Vulnerabilidad de PL / Java, que no tiene en cuenta los controles en objetos grandes. [11]

- CVE-2016-0773: Vulnerabilidad de PostgreSQL, que permite mediante uso de caracteres Unicode en una expresión regular causar denegación del servicio. [12]

- CVE-2016-1255: Vulnerabilidad derivada del script pg_cluster de algunas versiones de Linux, que permitía a usuarios locales, hacerse con privilegios de root, accediendo a un archivo de registro ubicado en /var/log/postgresql. [13]

- CVE-2016-2192: Vulnerabilidad PL /Java que permite a los usuarios autenticados editar asignaciones de tipos que no son de su propiedad. [14]

- CVE-2016-2193: Vulnerabilidad de PostgreSQL que no protege adecuadamente la seguridad de la fila en cache, lo que permite a los atacantes evadir las restricciones de una sesión abierta. [15]

---

[8] CVE-2015-7502 Vulnerabilidad 2015-7502, [En línea]. Disponible en: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7502 . [Accedido Octubre 2018]
[9] CVE-2016-0766 Vulnerabilidad 2016-0766, [En línea]. Disponible en: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0766 . [Accedido Octubre 2018]
[10] CVE-2016-0767 Vulnerabilidad 2016-0767, [En línea]. Disponible en: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0767 . [Accedido Octubre 2018]
[11] CVE-2016-0768 Vulnerabilidad 2016-0768, [En línea]. Disponible en: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0768 . [Accedido Octubre 2018]
[12] CVE-2016-0773 Vulnerabilidad 2016-0773, [En línea]. Disponible en: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0773 . [Accedido Octubre 2018]
[13] CVE-2016-1255 Vulnerabilidad 2016-1255, [En línea]. Disponible en: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1255 . [Accedido Octubre 2018]
[14] CVE-2016-2192 Vulnerabilidad 2016-2192, [En línea]. Disponible en: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2192 . [Accedido Octubre 2018]
[15] CVE-2016-2193 Vulnerabilidad 2016-2193, [En línea]. Disponible en: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2193 . [Accedido Octubre 2018]

- CVE-2016-5423: Vulnerabilidad de PostgreSQL que permite a usuarios remotos autenticados obtener información confidencial, denegación del servicio o ejecutar código arbitrario por medio de una expresión CASE. [16]

- CVE-2016-5424: Vulnerabilidad de PostgreSQL que permitía a usuarios remotos autenticados, con el rol CREATEDB O CREATEROLE, hacerse con permisos de superusuario con la utilización de comillas dobles (“), barra invertida (\), retorno de carro, caracteres de nueva línea. [17]

- CVE-2016-7048: El instalador de PostgreSQL, permitía a atacantes remotos ejecutar arbitrariamente código a través del uso de HTTP, mientras se descargaba el software. [18]

4.1 Aspectos a tener en cuenta para la seguridad de la base de datos PostgreSQL

Es necesario conocer e identificar algunos conceptos claves a tener en cuenta, para la implementación de seguridad informática

- Seguridad del Sistema Operativo: Su función es la de brindar protección, con el fin de cuidar los procesos, la información, los usuarios entre otros, normalmente se requiere de otro tipo de software como antivirus, que brinde protección contra virus, adware, troyanos y cryptovirus, adicional a esto es indispensable contar con un firewall, donde se establezcan políticas de acceso a los servicios que publica el sistema operativo. [19]

- Seguridad en la Red de Datos: Su objetivo es mantener el intercambio de información protegido y libre de riesgo, para ello utiliza herramientas como firewall, antispam, antimalware y filtrado de contenido. [20]

- Nivel de Autenticación para Usuarios: La autenticación se debe realizar mediante un usuario y contraseña, administrada por un sistema de Roles, que se utiliza para controlar el acceso a los objetos de la base de datos (Tablas, Secuencias, Vistas, Funciones). En el rol se define los privilegios

[16] CVE-2016-5423 Vulnerabilidad 2016-5423, [En línea]. Disponible en: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5423 . [Accedido Octubre 2018]
[17] CVE-2016-5424 Vulnerabilidad 2016-5424, [En línea]. Disponible en: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5424 . [Accedido Octubre 2018]
[18] CVE-2016-7048 Vulnerabilidad 2016-7048, [En línea]. Disponible en: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7048 . [Accedido Octubre 2018]
[19] BLOG.UTP. Seguridad y protección de los sistemas operativos, [En línea]. Disponible en: http://blog.utp.edu.co/seguridadso/ . [Accedido Octubre 2018]
[20] CERTSUPERIOR S DE RL DE CV. Seguridad en redes, [En línea]. Disponible en: https://www.certsuperior.com/SeguridadenRedes.aspx . [Accedido Octubre 2018]

sobre el contenedor de la BD o esquema al que cada usuario puede acceder. [21]

- Seguridad a Nivel de Esquemas: Un esquema es una sección dentro de la base de datos, que contiene los demás objetos de la BD como tablas, vistas, dominios, secuencias etc. Cuando se crea una BD se crea por defecto un esquema público, donde todos los usuarios pueden crear objetos en ella, por esta razón se debe definir al menos un esquema, donde se asignen los privilegios para cada grupo de usuarios. [22]

- Cifrado de Datos: PostgreSQL cuenta con soporte SSL (Secure Sockets Layer), que permite cifrar el tráfico entre los clientes o usuarios y el servidor, mediante una clave que cifra la conexión, para evitar que alguien pueda interceptar los datos que viajan a través de la conexión. [23]

- Seguridad de los Respaldos: PostgreSQL cuenta con múltiples herramientas para la realización de copias de seguridad, sin embargo, se debe contar con un esquema de tipo de respaldos, que permita controlar y evaluar la calidad de dichas copias, para que en el momento en que ocurra un incidente, se pueda recuperar y dar continuidad al negocio. [24]

- Seguridad a Nivel de Registros: PostgreSQL introdujo este mecanismo a partir de la versión 9.5, cuyo objetivo es definir condiciones que controlen la visibilidad de las filas a nivel de la tabla, actuando como filtro de la información. [25]

- Actualizaciones PostgreSQL: Es indispensable realizar todas las actualizaciones publicadas por el fabricante, ya que las mismas corrigen las vulnerabilidades reportadas y permite que el sistema cuente con nuevas características de rendimiento, robustez y soporte de la comunidad. [26]

---

[21] CLAVADETSCHER Charles. Autorización en PostgreSQL, 2015. [En línea]. Disponible en: http://www.schmiedewerkstatt.ch/documents/04-publications/autorizacion_en_postgresql_script_pdfa.pdf . [Accedido Octubre 2018]

[22] Ibid, pág 11

[23] EMC2NET. PostgreSQL y el uso de SSL, [En línea]. Disponible en: https://e-mc2.net/es/postgresql-y-el-uso-de-ssl . [Accedido Octubre 2018]

[24] TENER Simón, PEQUEÑO Nelson. Respaldo y recuperación de datos. 2000, [En línea]. Disponible en: https://es.slideshare.net/asaelito/respaldo-y-recuperacion-de-informacion . [Accedido Octubre 2018]

[25] CLAVADETSCHER Charles. OP CIT pág 49

[26] 2NDQUADRANT. Actualizar PostgreSQL, [En línea]. Disponible en: https://www.2ndquadrant.com/es/servicios/actualizar-postgresql/ . [Accedido Octubre 2018]

4.2 MARCO LEGAL

La constitución política colombiana, es la carta magna que contiene los derechos y deberes que garantizan el orden económico, político y social en nuestra sociedad, en ese orden es necesario mencionar el artículo que protege la intimidad personal y de la información.

- **Artículo 15:** Este artículo protege el derecho a la intimidad personal y familiar, así como a conocer, rectificar y actualizar información recolectada sobre ella en bancos de datos o archivos de entidades privadas y públicas.

4.2.1 Normatividad en Colombia, ley 1273 de 2009 "Delitos Informáticos en Colombia"

Esta ley modificó el código penal, creando un nuevo bien tutelado llamado "de la protección de la información y de los datos", que incluye los siguientes capítulos.

- Capítulo Primero: Define los atentados contra la confidencialidad, integridad, y disponibilidad de los datos y de los sistemas informáticos [27], el cual se compone de los siguientes artículos:

  Artículo 269A. Acceso Abusivo a un Sistema Informático: Este artículo condena a la persona que sin autorización ingrese total o parcialmente a un sistema informático protegido o no.

  Artículo 269B. Obstaculización Ilegítima de Sistema Informático o Red de Telecomunicación: Condena a la persona que obstruya el acceso a un sistema informático, datos o red de telecomunicaciones.

  Artículo 269C. Interceptación de Datos Informáticos: Condena a la persona que sin orden judicial intercepte datos en el origen o destino, de un sistema informático o las emisiones electromagnéticas.

  Artículo 269D. Daño Informático: Condena a la persona que sin ser su función, destruya, dañe deteriore, borre, cambie o suprima datos informáticos.

  Artículo 269E. Uso de Software Malicioso: Condena a la persona que produzca, adquiera, trafique, distribuya, venda programas de computación dañinos.

[27] EL CONGRESO DE COLOMBIA. Ley 1273 de 2009, [En línea]. Disponible en: http://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf . [Accedido Octubre 2018]

Artículo 269F. Violación de Datos Personales: Condena a la persona que sin autorización y para su provecho o de un tercero, obtenga, sustraiga, ofrezca, venda datos personales contenidos en archivos, base de datos u otros.
Artículo 269G. Suplantación de Sitios Web para Capturar Datos Personales: Condena a la persona que diseñe, desarrolle, programe o envíe páginas electrónicas o enlaces con el fin de obtener datos personales.

Artículo 269H. Circunstancias de Agravación Punitiva: Las penas se aumentan de la mitad a las tres cuartas partes si la conducta es:

- sobre redes, sistemas informáticos o comunicaciones estatales,
- Ser servidor público en ejercicio de sus funciones
- Abuzo de confianza del poseedor de la información
- Revelar información en perjuicio de otro
- Para fines terroristas o que genere riesgo para la seguridad nacional.

- Capitulo Segundo: Define otras infracciones como hurto por medios informáticos y transferencia no consentida de activos [28], el cual se compone de los siguientes artículos:

  Artículo 269I. Hurto por Medios Informáticos y Semejantes: Condena a la persona que viole los sistemas de seguridad, y realice la conducta del artículo 239, manipulando el sistema informático, o red electrónica, telemática.

  Artículo 269J. Transferencia no Consentida de Activos: Condena a la persona que con ánimo de lucro y utilizando algún sistema informático transfiera de manera no consentida algún activo, perjudicando un tercero.

Ley 599 de 2000, Código Penal Colombiano

El título III de la presente ley reglamenta la conducta punible

- Artículo 19. Delitos y Contravenciones: El estado dividió las conductas punibles en delitos y contravenciones.

- Artículo 20. Servidores Públicos: Son servidores públicos los empleados del estado y las entidades descentralizadas, así como los miembros de las corporaciones públicas.

[28] Ibid, pág 3

- Artículo 21. Modalidades de la Conducta Punible: Esta se divide en dolosa, culposa o preterintencional.

- Artículo 22. Dolo: Se presenta dolo cuando el agente conoce los hechos constitutivos de la infracción penal y quiere su realización.

- Artículo 23. Culpa: Se constituye la culpa cuando el resultado de la infracción se da por no tener el cuidado o habiéndolo previsto confió en poder evitarlo.

- Artículo 24. Preterintencional: Cuando el resultado de la conducta siendo previsible, excede la intención del infractor. [29]

Ley Estatutaria 1266 de 2008

Esta ley reglamenta las disposiciones generales del hábeas data, manejo de la información contenida en las bases crediticias, financieras comerciales y de servicios.

- Artículo 3. Definiciones:
    - Titular de la información: Es la persona jurídica o natural cuya información reposa en un banco de datos sujeta al derecho de hábeas data y demás garantías.

    - Fuente de Información: Organización persona o entidad que recibe los datos personales de los titulares de la información, por una relación comercial o de servicio y que con autorización del titular se suministra a un operador de información.

    - Operador de Información: Organización persona o entidad que recibe datos personales, los administra y los pone en conocimiento de los usuarios bajo los parámetros de la presente ley.

    - Usuario: Es la persona natural o jurídica que, en los términos previstos por la presente ley, puede acceder a la información de uno o varios titulares suministrada por el operador de la fuente.

    - Dato Personal: Es cualquier información vinculada a una o varias personas los cuales se clasifican en públicos, semiprivados o privados.

[29] EL CONGRESO DE COLOMBIA. Ley 599 de 2000, [En línea]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html. [Accedido Noviembre 2019]

- Dato Público: Son públicos los datos presentes en documentos públicos, sentencias judiciales, que no gocen de reserva y el estado civil de las personas.

- Dato Semiprivado: Es el dato que no tiene naturaleza reservada, íntima, ni pública, cuya divulgación o conocimiento puede interesar a cierto sector o grupo como datos crediticios o financieros.

- Dato Privado: Es todo dato que por su naturaleza reservada o íntima sólo es relevante para el titular

- Artículo 5. Circulación de la Información: La información administrada por los operadores que haga parte del banco de datos, podrá ser entregada de manera escrita o verbal a las siguientes personas y en los siguientes términos:
  - A los titulares, a las personas autorizadas por estos o a sus causahabientes.

  - A los usuarios de la información con base en los parámetros de la presente ley.

  - A cualquier autoridad judicial previa orden judicial.

  - A las entidades públicas del poder ejecutivo, para el cumplimiento de alguna de sus funciones

  - A los órganos de control cuando la información sea necesaria para una investigación en curso [30]

Ley Estatutaria 1581 de 2012.

- Artículo 4. Principios para el Tratamiento de Datos Personales
  - Principio de Legalidad en Materia de Tratamiento de Datos: Es una actividad reglada y debe estar sujeta a lo establecido en ella y las demás disposiciones.

  - Principio de Finalidad: El tratamiento debe tener una finalidad legítima acorde a la constitución y la ley y debe ser informada a la ley.
  - Principio de Libertad: El tratamiento solo puede ser ejercido con el consentimiento expreso y previo del titular

[30] EL CONGRESO DE COLOMBIA. Ley Estatutaria 1266 de 2008, [En línea]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html#1. [Accedido Noviembre 2019]

- Principio de Veracidad o Calidad: La información debe ser veraz exacta, comprobable y comprensible, se prohíbe el tratamiento de datos incompletos o parciales que induzcan a error.

- Principio de Transparencia: Se debe garantizar al titular de la información por parte del encargado del tratamiento, información acerca de la existencia de datos que le conciernan.

- Principio de Acceso y Circulación Restringida: El tratamiento sólo puede hacerse por personas autorizadas por el titular o por personas previstas en la presente ley.

- Principio de Seguridad: La información debe ser manejada con las medidas técnicas administrativas y humanas necesarias para brindar seguridad a los registros con el fin de evitar su pérdida, adulteración o consulta no autorizada.

- Principio de Confidencialidad: Se debe garantizar la reserva de todos los datos que no tengan la naturaleza de públicos, por las personas que intervienen en el tratamiento de datos. [31]

Decreto 2693 de 2012.

- Artículo 7. Modelo de Gobierno en Línea:
  - Información en Línea: La misión, planeación estratégica, trámites y servicios y demás información deben estar disponibles en línea, cumpliendo todos los requisitos de disponibilidad, calidad, accesibilidad y estándares de seguridad.

  - Interacción en Línea: Se deben habilitar herramientas de comunicación de doble vía entre los ciudadanos y los servidores públicos, así mismo se deben habilitar servicios de consulta en línea, que acerquen a los usuarios a la administración.

  - Transacción en Línea: Los obligados deben disponer de trámites y servicios para que los ciudadanos puedan realizar desde la solicitud hasta la obtención del servicio sin ser necesario que aporten documentos que reposen en cualquier entidad pública.

[31] EL CONGRESO DE COLOMBIA. Ley Estatutaria 1581 de 2012, [En línea]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html#CAP%C3%8DTULO%20I-VII [Accedido Noviembre 2019]

- Transformación: Los obligados deben eliminar límites entre dependencias y otras entidades públicas, intercambiando información entre ellas.

- Democracia en Línea: Los obligados desarrollan un ambiente para motivar a los ciudadanos en el proceso de toma de decisiones de un estado integrado totalmente en línea.

- Elementos Transversales: Los obligados identifican los diferentes tipos de usuarios, sus necesidades e investigan las tendencias de comportamiento. [32]

Ley 1712 de 2014.

- Artículo 24. Del Derecho de Acceso a la Información: Toda persona puede solicitar y recibir información del sujeto obligado tal cual lo establece la ley y la constitución.

- Artículo 25. Solicitud de Acceso a la Información Pública: Cualquier persona tiene derecho a solicitar información de forma verbal o escrita

- Artículo 26. Respuesta a Solicitud de Acceso a la Información: Es el acto mediante el cual, de manera oportuna, completa, veraz, actualizada y motiva, la parte obligada responde a la persona una solicitud de acceso a la información pública. [33]

4.3 MARCO CONCEPTUAL

Para llevar a cabo la realización de un procedimiento, que mitigue el riesgo de intrusión a las bases de datos PostgreSQL familia 9.x, es necesario entender y conocer los conceptos que actuarán como base, para la construcción de lo señalado.

4.3.1 Términos

A continuación se describe detalladamente los elementos que permiten el entendimiento de los conceptos abordados en este estudio:

- Vulnerabilidad: es la falta de resistencia, al presentarse una amenaza o

[32] MINISTERIO DE LAS TIC. Decreto 2693 de 2012, [En línea]. Disponible en: https://www.mintic.gov.co/portal/604/articles-3586_documento.pdf. [Accedido Noviembre 2019]
[33] EL CONGRESO DE COLOMBIA. Ley 1712 de 2014, [En línea]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1712_2014.html. [Accedido Noviembre 2019]

incapacidad de reponerse después que se presenta un desastre, teniendo presente que se pueden presentar factores internos o externos, con diferentes niveles de daños. [34]

- Postgresql: Es un sistema de gestión de base de datos, que pertenece a la categoría de base de datos relacionales, es orientada a objetos y su uso es libre [35]

- Riesgo: Probabilidad existente de que un hecho ocurra y produzca una serie de efectos que afectan una actividad. [36]

- Amenaza: Toda acción o elemento apto que atenta contra la seguridad de la información, esta surge a partir de la existencia de una o más vulnerabilidades. [37]

- Base de Datos: Es un conjunto de datos, que por su origen hacen parte de un mismo contexto, los cuales son almacenados de manera sistemática, para su posterior consulta o uso. [38]

- Red de Datos: Es un conjunto de computadores conectados entre ellos, a través de dispositivos físicos que reciben o envían ondas electromagnéticas, impulsos eléctricos u otro medio que transporte datos, con el fin de compartir información, servicios u otro tipo de recurso. [39]

- Router: Dispositivo cuya tarea es la de proporcionar conectividad y administrar el tráfico de la información que viaja por una red de datos, ofreciendo internet por medio de ADSL, cable o wifi, adicional a esto cuenta con protección de firewall, que permite la administración en el ámbito de la seguridad. [40]

---

[34] UNISDR.ORG. ¿Qué significa vulnerabilidad?, [En línea]. Disponible en: https://www.unisdr.org/2004/campaign/booklet-spa/page8-spa.pdf. [Accedido Octubre 2018]

[35] PLATZI. ¿Qué es PostgreSQL y cuáles son sus ventajas?, [En línea]. Disponible en: https://platzi.com/blog/que-es-postgresql/ . [Accedido Octubre 2018]

[36] EPN. Riesgo, Amenaza y Vulnerabilidad, [En línea]. Disponible en: http://epn.gov.co/elearning/distinguidos/SEGURIDAD/13_riesgo_amenaza_y_vulnerabilidad.html . . [Accedido Octubre 2018]

[37] Universidad Nacional de Luján. Amenazas a la seguridad de la información, [En línea]. Disponible en: http://www.seguridadinformatica.unlu.edu.ar/?q=node/12 . [Accedido Octubre 2018]

[38] ECURED. Bases de Datos, [En línea]. Dsiponible en: https://www.ecured.cu/Bases_de_datos . [Accedido Octubre 2018]

[39] SEARCHDATACENTER. Networking, redes, cableado.. similitudes y diferencias, [En línea]. Disponible en: https://searchdatacenter.techtarget.com/es/consejo/Networking-redes-cableado-similitudes-y-diferencias . [Accedido Octubre 2018]

[40] TECNOLOGÍA-INFORMÁTICA. ¿Qué es un router?, [En línea]. Disponible en: https://tecnologia-informatica.com/que-es-router-wifi-comprar-ampliar-alcance/ . [Accedido Octubre 2018]

- Firewall: Es una defensa que actúa contra gusanos, troyanos, virus informáticos y ataques de fuerza bruta, se puede encontrar como hardware (enrutador) o software (programa de seguridad), pero en ambos casos su función es analizar el tráfico entrante para asegurarse de que no contenga ningún elemento malicioso o tráfico inusual [41]

- Sistema Operativo: Es el principal software de un computador, cuya función es suministrar una interfaz entre los demás programas, hardware y usuario, proporcionando una serie de elementos como directorios, archivos, unidades, etc, existen diversos tipos de sistemas operativos, entre los que tenemos, Windows, Linux, Mac OS entre otros. [42]

- Hacker: Persona que posee conocimientos avanzados en informática con capacidad de realizar actividades desafiantes e ilícitas desde un computador, sin embargo, existen varias comunidades de hacker, dependiendo de su intención o finalidad, dentro de los cuales encontramos el hacker de sombrero blanco, encargados de los sistemas informáticos cuya función principal es buscar vulnerabilidades con el fin de corregirlas y así proteger la información de intrusos, hacker de sombrero gris, que traspasan los niveles de seguridad para luego ofrecer sus servicios y hacker de sombrero negro que violentan los sistemas de seguridad para extraer información con un fin monetario. [43]

- Ataque Informático: Es una actividad hostil contra un sistema, utilizando una serie de herramientas informáticas cuyo objetivo es explotar una serie de vulnerabilidades presentes en los sistemas, mediante esta acción el atacante desea lograr un beneficio. [44]

4.3.2 Tipo de Vulnerabilidades

A continuación se enumeran los tipos de debilidades, que permite que un atacante pueda comprometer la seguridad de un sistema

- Privilegios excesivos: No se deben entregar privilegios o permisos, que

[41] LATAM-KASPERSKY. ¿Qué es un firewall?, [En línea]. Disponible en: https://latam.kaspersky.com/resource-center/definitions/firewall . [Accedido Octubre 2018]
[42] SOFTWAREDOIT. Definición términos de software, [En línea]. Disponible en: https://www.softwaredoit.es/definicion/index.html . [Accedido Octubre 2018]
[43] VIX. ¿Qué es un hacker?, [En línea]. Disponible en: https://www.vix.com/es/btg/tech/13182/que-es-un-hacker . [Accedido Octubre 2018]
[44] CONSULTHINK.IT. ¿Qué es y en qué consiste un ataque informático?, [En línea]. Disponible en: https://consulthink.it/es/que-es-y-en-que-consiste-un-ataque-informatico/ . [Accedido Octubre 2018]

excedan los requisitos de las funciones del cargo [45]

- Abuso de privilegios: Esta vulnerabilidad se materializa cuando un usuario sustrae información a la cual tiene acceso para cumplir con sus funciones, para lucrarse de ella. [46]

- Vulnerabilidades de la plataforma: Los sistemas operativos son los que más aportan a este tipo de riesgos, debido a las diferentes arquitecturas y versiones utilizadas para alojar las bases de datos. [47]

- Inyección SQL: Esta vulnerabilidad se hizo popular con la entrada de las aplicaciones web, que ofrecen páginas dinámicas para almacenar información, en donde un usuario con privilegios elevados, utiliza procedimientos almacenados, para realizar consultas no autorizadas. [48]

4.3.3 Ataques Informáticos

A continuación se enumeran y describen los ataques y elementos utilizados para comprometer un sistema

- Malware: Software malicioso cuya finalidad es infiltrarse en cualquier sistema, con el fin de dañarlo. [49]

- Virus: Programas con código maligno que busca infectar los archivos del sistema con el fin de modificarlo o dañarlo, es necesario que el usuario lo ejecute para que se pueda propagar. [50]

- Gusanos: Programa de software que puede replicarse así mismo entre ordenadores o a través de la red de datos, provocando niveles de destrucción elevados. [51]

---

[45] ONA SYSTEMS. Vulnerabilidades importantes que afectan la seguridad de bases de datos en las empresas, [En línea]. Disponible en: https://www.onasystems.net/vulnerabilidades-importantes-afectan-la-seguridad-bases-datos-las-empresas/ . [Accedido Octubre 2018]

[46] id

[47] id

[48] id

[49] AVAST. Malware & Antimalwalre, [En línea]. Disponible en: https://www.avast.com/es-es/c-malware . [Accedido Octubre 2018]

[50] INFOSPYWARE. ¿Qué son los virus informáticos?, [En línea]. Disponible en: https://www.infospyware.com/articulos/%C2%BFque-son-los-virus-informaticos/ . [Accedido Octubre 2018]

[51] KASPERSKY. Gusanos informáticos, [En línea]. Disponible en: https://www.kaspersky.es/resource-center/threats/viruses-worms . [Accedido Octubre 2018]

- Troyanos: Tomó su nombre de la historia, del caballo de madera utilizado para engañar a los defensores de troya, para poder introducir soldados en la ciudad, como su nombre lo indica, oculta software malicioso dentro de un archivo aparentemente normal, con el fin de controlar el equipo infectado y robar datos. [52]

- Spyware: Software espía, cuya finalidad es la de recopilar información de un ordenador y transmitirla a un medio externo sin permiso del propietario del ordenador, adicional a esto también muestra anuncios sin ser solicitados, (pop-up), redirecciona páginas web e instala marcadores de teléfono. [53]

- Adware: Software diseñado para mostrar anuncios de publicidad, normalmente mediante navegadores, considerado como un programa potencialmente no deseado. [54]

- Ransonware: Software malicioso que, al momento de infectar el computador, le da al atacante la capacidad de bloquear y encriptar la información, desde una ubicación remota, para pedir un rescate con el fin de devolver dicha información. [55]

- Phishing: Técnica de ingeniería social cuya función es obtener datos confidenciales como usuario, contraseña, datos de tarjetas de crédito, para hacerse pasar por una comunicación legitima y confiable. [56]

- Denegación de Servicio Distribuido (DDoS): Es uno de los ataques más temidos ya que es fácil de realizar, económicamente hablando y es difícil de rastrear, su contundencia se debe a que no intenta penetrar los niveles de seguridad que protegen el servidor sino bloquearlo, consiste en realizar una gran cantidad de peticiones al servidor hasta que este colapse.

---

[52] CO.NORTON. ¿Qué es un troyano?, [En línea]. Disponible en: https://co.norton.com/internetsecurity-malware-what-is-a-trojan.html . [Accedido Octubre 2018]

[53] CISET. Spyware-programa espía, [En línea]. Disponible en: https://www.ciset.es/glosario/488-spyware . [Accedido Octubre 2018]

[54] MALWAREBYTES. ¿Qué es el adware?, [En línea]. Disponible en: https://es.malwarebytes.com/adware/ . [Accedido Octubre 2018]

[55] PANDASECURITY. ¿Qué es un ransomware?, [En línea]. Disponible en: https://www.pandasecurity.com/spain/mediacenter/malware/que-es-un-ransomware/ . [Accedido Octubre 2018]

[56] SEGU-INFO. Phishing, [En línea]. Disponible en: https://www.segu-info.com.ar/malware/phishing.htm . [Accedido Octubre 2018]

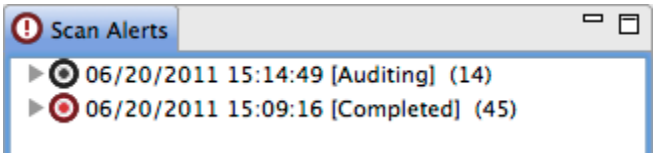
4.3.4 Herramientas para Escanear Vulnerabilidades a Base de Datos

En la actualidad existe un sin número de herramientas especializadas en realizar escaneo de vulnerabilidades en sistemas operativos y bases de datos, que brindan información detallada para llevar a cabo pruebas de pent test, con el fin de evaluar la seguridad con que cuenta el sistema operativo, aplicación web o base de datos, estas mismas herramientas son utilizadas por los intrusos para llevar a cabo ataques dirigidos a estos sistemas de información.

- VEGA: Herramienta escrita en java con entorno disponible para Linux, mac y Windows, su funcionalidad principal es encontrar SQL injection, header injection, directory listing, Shell injection, cross site scripting y file inclusión.

  Vega iniciará el escaneo de la aplicación enviando muchas peticiones, para que el motor de rastreo realice pruebas en cada ruta, para determinar si es un archivo o directorio, Vega empezará a mostrar alertas con los enlaces o rutas vistas o rastreadas, a continuación en la figura 1 se muestra los tipos de alerta que el programa vega puede detectar.

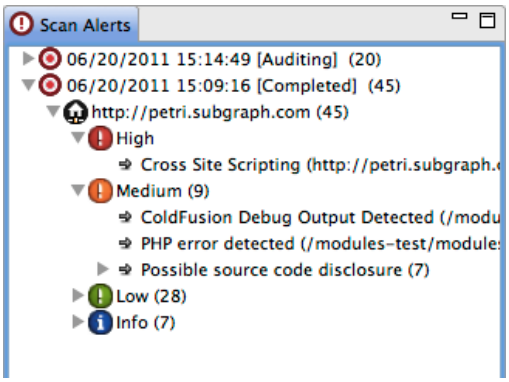
  Figura 1. Scan Alerts programa Vega

  Fuente: SUBGRAPH. Vega lo ayuda a encontrar y reparar secuencias de comandos, [En línea]. Disponible en https://subgraph.com/vega/ [Accedido Noviembre 2018]
  Mientras avanza la exploración aparecerán otras instancias de alertas que revelan vulnerabilidades encontradas, Clasificándolas por niveles de seguridad, tipo e instancias

  Así mismo en la figura 2, observamos las vulnerabilidades encontradas por el programa vega

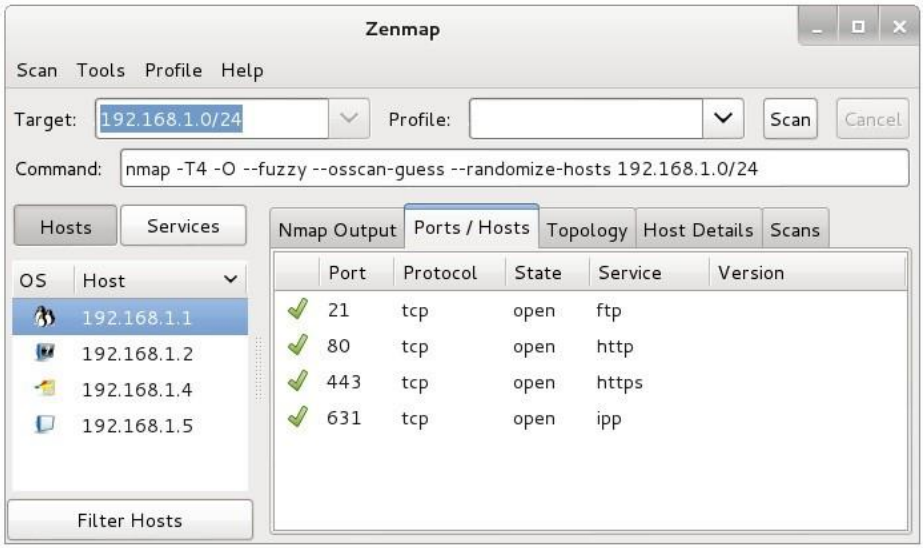
Figura 2. Vulnerabilidades encontradas



Fuente: SUBGRAPH. Vega lo ayuda a encontrar y reparar secuencias de comandos, [En línea]. Disponible en https://subgraph.com/vega/ [Accedido Noviembre 2018]

- NMap: Herramienta gratis de código abierto, para realizar exploraciones de red y/o auditorias de seguridad, que utiliza los paquetes IP, para encontrar los hosts que están disponibles en la red, servicios, versión del sistema operativo, tipo de filtros o cortafuegos en uso. La figura 3 se muestra una exploración en la red de datos 192.168.1

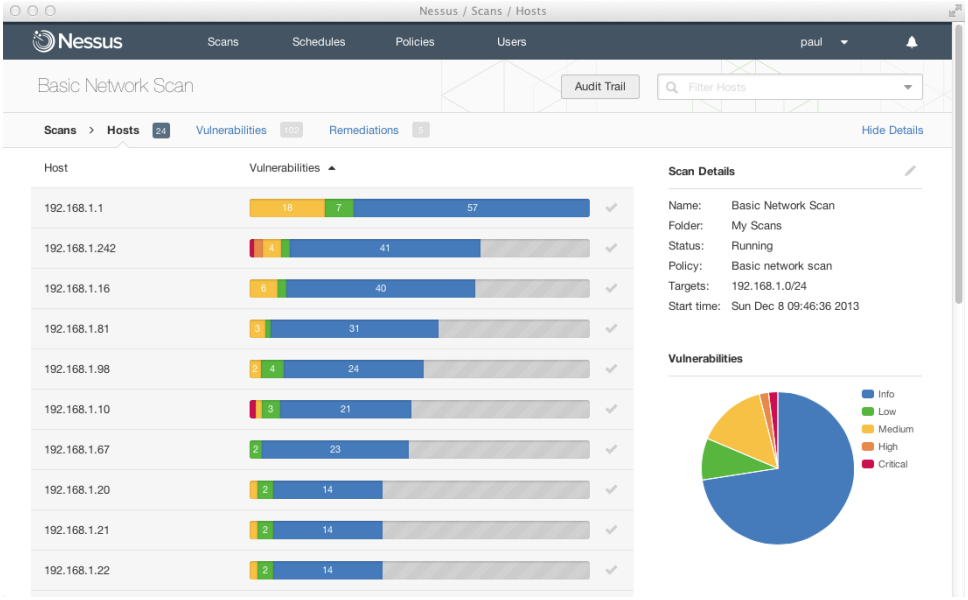
Figura 3. Exploración NMap



Fuente: WELIVESECURITY. Ofuscación de redes informáticas: dificultando ataques exploratorios, [En línea]. Disponible en https://www.welivesecurity.com/la-es/2014/09/29/ofuscacion-de-redes-dificultando-ataques/ [Accedido Mayo 2020]

- Nessus: Utilizado en más de 75.000 organizaciones en todo el mundo, es una herramienta de auditoría, que busca fallas críticas de seguridad, en la figura 4 se muestra una exploración de vulnerabilidades en una red de datos.

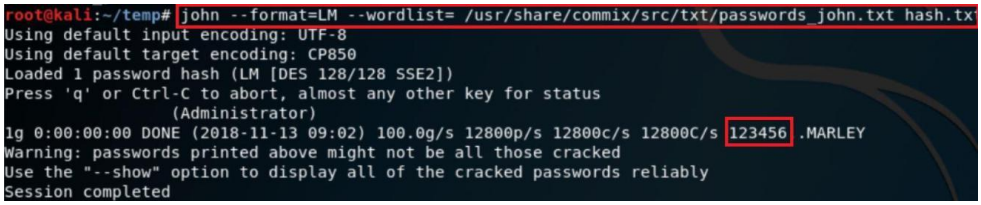
Figura 4. Exploración Vulnerabilidades



Fuente: BLACKDARKO. Recuperar contraseña nessus, [En línea]. Disponible en https://blackdarko.wordpress.com/2017/01/25/recuperar-contrasena-nessus/ [Accedido Mayo 2020]

- John the Ripper: Herramienta de descifrado de contraseña para probar la fortaleza de contraseñas, también puede ser usada para encontrar la contraseña de un sistema e ingresar en él, es compatible con ataque de diccionario y de fuerza bruta, en la figura 5, se observa un ataque de diccionario donde la contraseña del sistema operativo es 123456

Figura 5. Ataque de diccionario

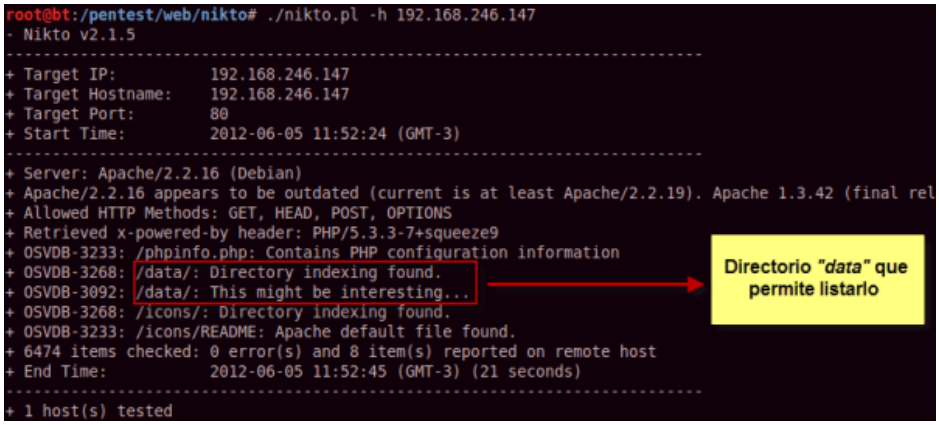


Fuente: NOTICIASSEGURIDAD. John the ripper-crackear contraseñas de windows, [En línea]. Disponible en

https://noticiasseguridad.com/tutoriales/john-the-ripper-crackear-contrasenas-de-windows/ [Accedido Mayo 2020]

- Nikto: Software de código abierto, diseñado para escanear y encontrar vulnerabilidades en los servidores web, permite detectar más de 3200 archivos potencialmente peligrosos, a continuación la figura 6 muestra como nikto detecta que el servidor web 192.168.246.147 permite listar el directorio data.

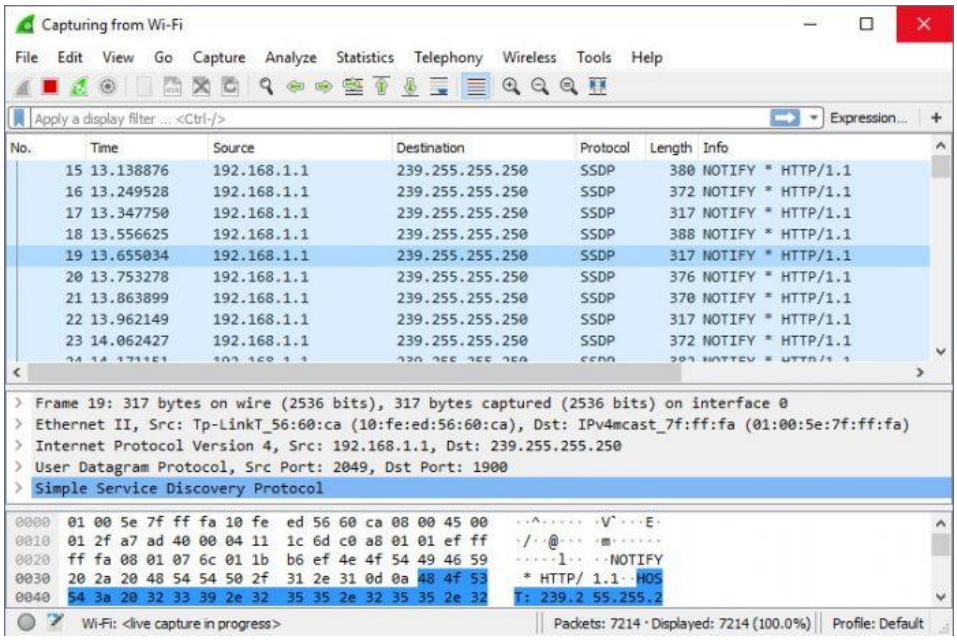
Figura 6. Exploración de un servidor web



Fuente: WELIVESECURITY. Auditando un servidor web con nikto, [En línea]. Disponible en https://www.welivesecurity.com/la-es/2012/06/05/auditando-servidor-web-nikto/ [Accedido Mayo 2020]

- Wireshark: Analizador de protocolos de red o sniffer, cuya función es capturar y navegar por los contenidos de los paquetes capturados, en la figura 7 se observa la captura de tráfico dentro de una red de datos.

Figura 7. Captura de tráfico

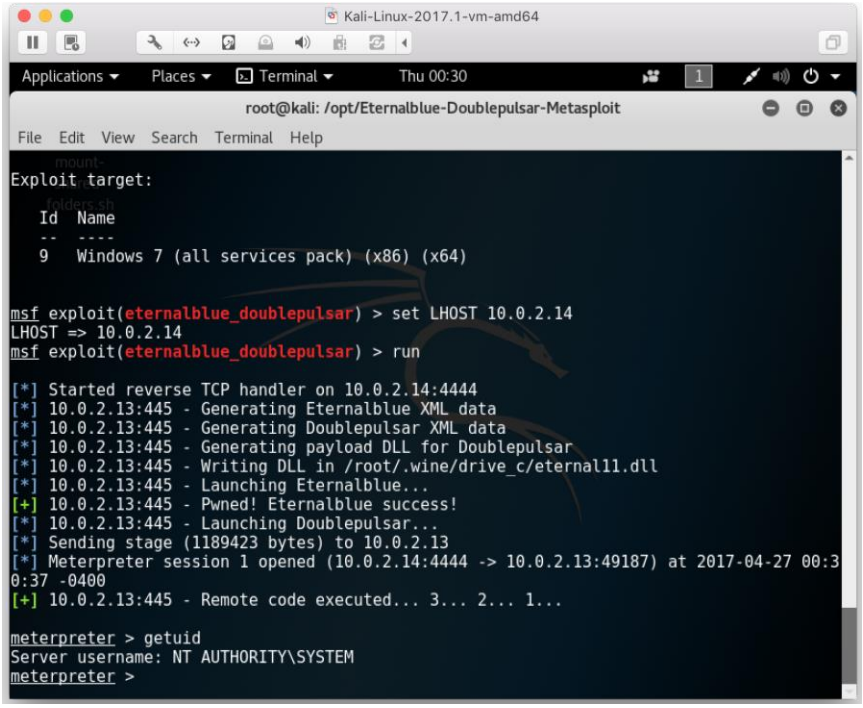


Fuente: HACKERSFUN. Wireshark 3 ya disponible, [En línea]. Disponible en https://hackersfun.com/wireshark-3-ya-disponible/ [Accedido Mayo 2020]

- Metasploit: Proporciona información de las vulnerabilidades, ayudando en las pruebas de pent test y en la ejecución y explotación de las vulnerabilidades de seguridad, [57] en la figura 8 se observa el uso de un exploid para acceder a un sistema operativo Windows.

[57] CAPACITY. Las 8 mejores herramientas de seguridad y hacking, [En línea]. Disponible en http://blog.capacityacademy.com/2012/07/11/las-8-mejores-herramientas-de-seguridad-y-hacking/ [Accedido Noviembre 2018]

Figura 8. Corriendo exploid eternalblue_doublepulsar



Fuente: MEDIUM. Hackea Windows con kali, metasploit y fuzzbunch [En línea]. Disponible en https://medium.com/@acheca/hackea-windows-con-kali-metasploit-y-fuzzbunch-f3d6a4153050 [Accedido Mayo 2020]

- SQLMap: Es una herramienta automatizada de inyección ciega de sql, permite generar una huella digital en el sistema de base de datos, tiene soporte para múltiples bases de datos como: Mysql, Oracle, Postgresql, Sql server, Acceses, Firebird entre otros, igualmente soporta las siguientes técnicas: ciego basado en el tiempo, ciego basado en booleano, basado en el error, consultas apiladas y consulta de unión, [58] en la figura 9 se observa como mediante la herramienta sqlmap, se puede acceder a ver la estructura de la table user de la DB bwapp.

[58] GITHUB. Características SQLMap, [En línea]. Disponible en: https://github.com/sqlmapproject/sqlmap/wiki/Features [Accedido Noviembre 2018]

Figura 9. Lista de columnas de la tabla user DB bwapp

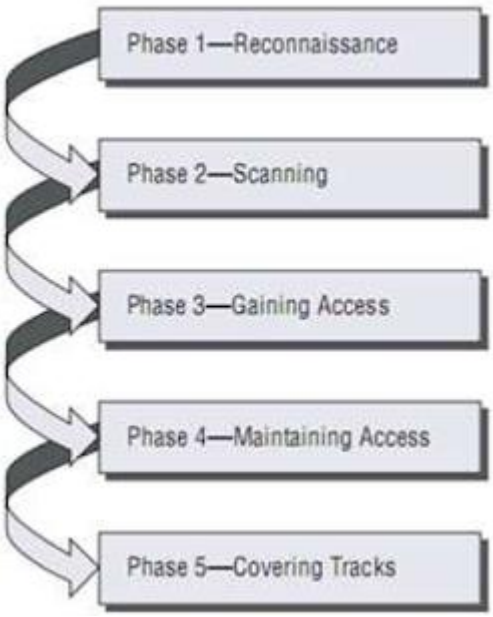
```
[15:59:59] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.10
back-end DBMS: MySQL >= 5.0.0
[15:59:59] [INFO] fetching columns for table 'users' in database 'bwapp'
Database: bwapp
Table: users
[9 columns]
+-----------------+--------------+
| Column          | Type         |
+-----------------+--------------+
| activated       | tinyint(1)   |
| activation_code | varchar(100) |
| admin           | tinyint(1)   |
| email           | varchar(100) |
| id              | int(10)      |
| login           | varchar(100) |
| password        | varchar(100) |
| reset_code      | varchar(100) |
| secret          | varchar(100) |
+-----------------+--------------+
```

Fuente: 10DEGRES. Sqlmap, [En línea]. Disponible en http://10degres.net/sqlmap/ [Accedido Mayo 2020]

4.3.5 Anatomía de un Ataque Informático

Para aprender a pensar como lo hacen los atacantes, es necesario conocer que etapas conforman un ataque, por tanto es necesario analizar y comprender la forma como los atacantes planean y ejecutan un ataque, en la figura 10 se observa la anatomía de un ataque informático.

Figura 10. Etapas de un ataque informático



Fuente: MSNSEGURIDAD. Anatomía de un Ataque Informático, [En línea]. Disponible en: http://msnseguridad.blogspot.com/2012/08/anatomia-de-un-ataque-informatico.html. [Accedido Noviembre 2018]

- Fase 1 Reconocimiento: En esta etapa se obtiene la información de la potencial víctima, que puede ser una organización o una persona, en esta etapa se utilizan recursos de internet como google y técnicas como la ingeniería social, dumpster diving que es la búsqueda de información en la papelera de reciclaje y el sniffing que consiste en escuchar todo lo que circula por la red.

- Fase 2 Exploración: En esta etapa se utiliza la información recolectada en la fase 1 para ahondar y tratar de conseguir más información como sistema operativo, nombre de host, direcciones IP e información de autenticación.

- Fase 3 Obtener Acceso: En esta etapa se materializa el ataque por medio de la explotación de las vulnerabilidades y fallos del sistema, encontradas durante las fases de reconocimiento y exploración, durante esta etapa se pueden presentar ataques de desbordamiento de buffer, denegación de servicio, distribución de denegación de servicio, filtrado de contraseñas y secuestro se sesión.

- Fase 4 Mantener el acceso: Cuando el atacante ha conseguido acceder al sistema, buscará instalar herramientas como backdoors, rootkits y troyanos, que le permitan acceder nuevamente desde cualquier parte donde tenga acceso a internet.

- Fase 5 Borrar Huellas: Una vez el atacante logra acceder e implantar las herramientas para mantener el acceso, intentará borrar las huellas para evitar ser detectado por el profesional de seguridad o administrador de la red, eliminando los archivos log del registro y las alarmas del sistema de detección de intrusos (IDS) [59]

4.3.6 Actualizaciones de Seguridad en PostgreSQL

PostgreSQL define las actualizaciones de dos formas, actualizaciones menores y actualizaciones mayores, en las actualizaciones menores se aplican parches y correcciones de seguridad, que no afectan el core del software, las actualizaciones

[59] MSNSEGURIDAD. Anatomía de un Ataque Informático, [En línea]. Disponible en: http://msnseguridad.blogspot.com/2012/08/anatomia-de-un-ataque-informatico.html. [Accedido Noviembre 2018]

mayores, si afectan el core y debe haber una adaptación de la base de datos al nuevo (Release)

Las actualizaciones menores se realizan desde las mismas terminales y no se corre riesgo, para el caso de las actualizaciones mayores si se debe tener cuidado, ya que debe haber una transición del clúster viejo de la BD al nuevo cluster. [60]

A continuación, se describe el proceso que se debe realizar, para instalar una actualización menor en PostgreSQL,

- Descargar paquete: Se debe descargar el último paquete de actualización disponible para la versión instalada

- Compilar e instalar: compilar dependiendo del sistema operativo y/o distribución e instalar la actualización

- Reiniciar el servidor: una vez se han instalado las actualizaciones menores, ya se puede contar con las nuevas herramientas, incluidas en la última versión de la actualización, pero la versión del servidor permanece en la anterior, hasta tanto no se reinicie. [61]

Tabla 1 Lanzamientos Actualizaciones Menores PostgreSQL

Versión	Menor actual	Soportado	Primer lanzamiento	Lanzamiento final
12	12,2	si	3 de octubre de 2019	14 de noviembre de 2024
11	11,7	si	18 de octubre de 2018	9 de noviembre de 2023
10	10.12	si	5 de octubre de 2017	10 de noviembre de 2022
9.6	9.6.17	si	29 de septiembre de 2016	11 de noviembre de 2021
9.5	9.5.21	si	7 de enero de 2016	11 de febrero de 2021
9.4	9.4.26	No	18 de diciembre de 2014	13 de febrero de 2020
9.3	9.3.25	No	9 de septiembre de 2013	8 de noviembre de 2018
9.2	9.2.24	No	10 de septiembre de 2012	9 de noviembre de 2017
9.1	9.1.24	No	12 de septiembre de 2011	27 de octubre de 2016
9.0	9.0.23	No	20 de septiembre de 2010	8 de octubre de 2015
8.4	8.4.22	No	1 de julio de 2009	24 de julio de 2014
8.3	8.3.23	No	4 de febrero de 2008	7 de febrero de 2013
8.2	8.2.23	No	5 de diciembre de 2006	5 de diciembre de 2011

[60] SYSADM. Actualizar PostgreSQL Versiones, [En linea]. Disponible en: https://sysadm.es/actualizar-postgresql-versiones-major/ [Accedido Diciembre 2018]
[61] TODOPOSTGRESQL. Actualización de PostgreSQL, [En línea]. Disponible en: https://todopostgresql.com/actualizacion-de-postgresql/ [Accedido Diciembre 2018]

Versión	Menor actual	Soportado	Primer lanzamiento	Lanzamiento final
8.1	8.1.23	No	8 de noviembre de 2005	8 de noviembre de 2010
8.0	8.0.26	No	19 de enero de 2005	1 de octubre de 2010
7.4	7.4.30	No	17 de noviembre de 2003	1 de octubre de 2010
7.3	7.3.21	No	27 de noviembre de 2002	27 de noviembre de 2007
7.2	7.2.8	No	4 de febrero de 2002	4 de febrero de 2007
7.1	7.1.3	No	13 de abril de 2001	13 de abril de 2006
7.0	7.0.3	No	8 de mayo de 2000	8 de mayo de 2005
6.5	6.5.3	No	9 de junio de 1999	9 de junio de 2004
6.4	6.4.2	No	30 de octubre de 1998	30 de octubre de 2003
6.3	6.3.2	No	1 de marzo de 1998	1 de marzo de 2003

Fuente: POSTGRESQL. Política de Versiones, [En línea]. Disponible en https://www.postgresql.org/support/versioning/ [Accedido Mayo 2020]

Los cambios más relevantes para cada versión, en cuanto a seguridad son las siguientes:

- Versión 12

    - Supervisión
        - Agrega contador de fallas de suma de control
        - Agrega seguimiento a objetos en la vista del sistema
        - Permite enumerar contenidos del directorio de archivo
        - Agrega la información del certificado del cliente a la vista en el sistema
        - Restringe la visibilidad de filas para los usuarios que no tienen privilegios
        - Al iniciar el servidor se emite un mensaje que incluye la versión del servidor
        - Informe de progreso

    - Autenticación
        - Soporte de cifrado GSSAPI
        - Verificación que el nombre de usuario de la DB, coincida con el nombre del certificado del cliente
        - Permite descubrir un servidor LDAP, manejando registros DNS SRV [62]

- Versión 11

    Esta corrección soluciona dos problemas de seguridad del servidor PostgreSQL, el primero se encontraba en los instaladores de Windows y el

[62] POSTGRESQL. E.3 Versión 12, [En línea]. Disponible en: https://www.postgresql.org/docs/12/release-12.html. [Accedido Mayo 2020]

segundo un paquete de más de 60 errores que habían sido informados los últimos tres meses.

- CVE-2019-10127: BigSQL el cual no elimina entradas de lista de acceso permisivas.

- CVE-2019-10128: EnterpriseDB no elimina entradas ACL permisivas.

- CVE-2019-10129: Divulgación de memoria al enrutar la partición, un usuario podía leer bytes de la memoria, ejecutando una instrucción INSERT en una tabla particionada.

- CVE-2019-10130: Se omiten políticas de seguridad de línea, un usuario podía ejecutar consultas SQL en una columna determinada con permisos de lectura, que creaban fugas que podían leer todos los datos en esa columna [63]

- Versión 10

  Se introduce el mecanismo de autenticación SCRAM, el cual define un protocolo de transmisión y almacenamiento de contraseñas seguro llamado SCRAM-SHA-256, el cual ofrece mayor seguridad en el método de autenticación por contraseña, reemplazando el anterior esquema, que estaba basado en MD5 [64]

- Versión 9.6

  Esta versión contiene las siguientes correcciones:

  - Quita el privilegio de ejecución de contrib, ya que es controlador obsoleto para el control de acceso.

  - Repara marcas de volatilidad en algunas funciones incorporadas, corrigiendo el catalogo inicial.
  - Corrige marcas de seguridad incorrectas, en las funciones incorporadas gin_clean_pending_list, brin_summarize_new_values, ts_rewrite, cursor_to_xml, ts_stat, cursor_to_xmlschema y binary_upgrade_create_empty_extension.

[63] UBUNLOG. Liberadas las nuevas versiones de PostgreSQL 11 [En línea]. Disponible en: https://ubunlog.com/liberadas-las-nuevas-versiones-de-postgresql-11-3-y-10-8-con-mas-de-60-errores-solucionados/. [Accedido Mayo 2020]

[64] POSTGRESQL. Comunicado de prensa para Postgres 10 [En línea]. Disponible en: https://www.postgresql.org/about/press/presskit10/es/. [Accedido Mayo 2020]

- Cambio del algoritmo ANALYZE, ya que anteriormente solo se hacía muestreo de una pequeña fracción de páginas, por lo que las tuplas no podían cambiar mucho.

- Corrección de una posible ejecución de ACTUALIZAR VISTA MATERIALIZADA, de manera concurrente.

- Corrección de la planificación de manera incorrecta de cláusulas de unión parametrizadas, que llevaban a una clasificación incorrecta de la condición de filtro.

- Se corrige el desbordamiento en bucles FOR, para PL/pgSQL [65]

- Versión 9.5
  Esta versión contiene las siguientes correcciones:
  - Repara marcas de volatilidad en algunas funciones incorporadas como cursor_to_xml, query_to_xml, cursor_to_xmlschema, query_to_xml_and_xmlschema y query_to_xmlschema.

  - Evita puntos muertos de comandos simultáneos CREATE INDEX CONCURRENTLY, que se ejecutan en transacciones REPEATABLE READ o SERIALIZABLE.

  - Se corrige la generación incorrecta de un plan de exploración de índice, cuando la columna de la tabla aparece en varias columnas de índice.

  - Se corrige las restricciones CHECK, que tienen subcláusulas NULL, las cuales son demostrables en condiciones AND/OR que podría permitir la exclusión de una tabla secundaria que no debe excluirse de la consulta.

  - Se corrigió bloqueo del ejecutor por la doble liberación en e l uso de GROUPING SET

  - Se evita la interrupción o cancelación de sesión, mientras se espera la confirmación de una transacción.

  - Se reduce el bloqueo durante la programación en el vacío automático. [66]

[65] POSTGRESQL. E.9 Versión 9.6 [En línea]. Disponible en: https://www.postgresql.org/docs/9.6/release-9-6-9.html. [Accedido Mayo 2020]

- Versión 9.4
  Esta versión contiene las siguientes correcciones:
  - Evita reutilizar los OID con las entradas TOAST eliminadas aun sin limpiar.
  - Se corrige la pérdida de memoria en consultas con combinaciones hash ejecutadas frecuentemente.
  - Evita la pérdida de referencia de un puntero cuando está activa la fila y se devuelve una tupla antigua.
  - Asegura que el nombre host se copie al copiar los datos de pg_stat_activityen la memoria.
  - Cuenta la cantidad de tuplas correctas durante la creación de un índice SP-GIST.
  - Cuenta la cantidad de tuplas correctas durante la creación de un índice GIST.
  - Evita el doble procesamiento de datos WAL, cuando se reinicia un walsender. [67]

- Versión 9.3
  Esta versión contiene las siguientes correcciones:
  - Solución de bloqueos en ecpg.
  - Se corrige el ecpg para que maneje correctamente las variables int y large, cuando se utiliza la compilación MSVC.
  - Se corrige el desbordamiento en bucles FOR, para PL/pgSQL.
  - Ajusta las pruebas de regresión PL/PYTON al pasar a Pyton 3.7
  - Admite pruebas para PL/PYTON, cuando se compila con pyton 3 y MSVC.
  - Cambia el nombre de funciones internas b64_decode y b64_encode, para evitar conflictos con las funciones Solaris 11.4

---

[66] POSTGRESQL. E.9 Versión 9.5 [En línea] Disponible en: https://www.postgresql.org/docs/9.5/release-9-5-13.html. [Accedido Mayo 2020]
[67] POSTGRESQL. E.9 Versión 9.4 [En línea]. Disponible en: https://www.postgresql.org/docs/9.4/release-9-4-18.html. [Accedido Mayo 2020]

- Sincroniza una copia de biblioteca con zonas horarias de IANA tzcode 2018e. [68]

4.3.7 Procedimiento para Prevenir Ataques DDoS

Este tipo de ataque, compromete el correcto funcionamiento del gestor de base de datos, ya que consiste en realizar una gran cantidad de peticiones al servidor hasta que este colapse, sin embargo existen técnicas que permiten prevenir y mitigar este tipo de ataques, estas herramientas permiten controlar y balancear las conexiones a la base de datos actuando como intermediario entre el servidor de aplicaciones y el servidor de base de datos.

Balanceador de Carga PGBouncer: Es un balanceador de carga que utiliza un sistema de hardware y software para administrar la cantidad de conexiones entrantes al servidor dividiendo de forma equitativa el trabajo entre los recursos disponibles, con esto se consigue controlar las solicitudes de acceso al servidor, para lo cual existen tres tipos de conexiones:

- **Pool de Sesiones:** Este tipo de conexión asigna una conexión a cada cliente, por el tiempo que dure la conexión.

- **Pool de Transacciones:** Este tipo de conexión asigna una conexión a cada transacción que se realice.

- **Pool de Sentencias:** En este caso se restringe la conexión a nivel de sentencias.

Este balanceador debe ser instalado entre el servidor de aplicaciones y el servidor de base de datos para que autorice o deniegue las conexiones que puedan ser atribuidas a un ataque DDoS. [69]

Tecnologías WAF: Web Application Firewall, son dispositivos de software o hardware, cuya función es proteger a los servidores web de tráfico malicioso, el WAF funciona como una medida preventiva para que el sitio web no quede fuera de línea o se infecte de código malicioso.

---

[68] POSTGRESQL. E.9 Versión 9.3 [En línea]. Disponible en: https://www.postgresql.org/docs/9.3/release-9-3-23.html. [Accedido Mayo 2020]

[69] LOPEZ Henry, PAREDES Oscar. Mitigación de Ataques DDoS en Base de Datos Mediante un Balanceador de Carga. [En línea]. Disponible en: https://journal.espe.edu.ec/ojs/index.php/geeks/article/download/278/257 . [Accedido Febrero 2019]

Los WAF fueron creados para analizar y comprender los tipos de datos que se permiten para cada protocolo http, smtp etc.
La solución WAF actúa como un muro entre la aplicación web y los visitantes para impedir que las solicitudes maliciosas afecten al sitio [70]
El sistema detecta los patrones de ataque a aplicaciones web de Cross-Site Scripting, inyección SQL, Cross-Site Request Forgery y Denegación de Servicio. [71]

4.3.8 Procedimiento para Prevenir Ataques por SQLInjection

Este tipo de ataque ocurre cuando datos no confiables llegan al intérprete como parte de una consulta o comando, para ejecutar comandos intencionados o acceder a datos no autorizados.
Características

- Los atacantes pueden ser internos, externos o administradores
- Cualquier fuente de datos, puede constituir un elemento para realizar inyección
- Este tipo de amenaza es común dentro de las aplicaciones web
- Es fácil de detectar
- Una inyección mal realizada, puede provocar daño o corrupción de datos

El origen de la vulnerabilidad radica en el chequeo o filtrado incorrecto de variables que utilizan las aplicaciones y que bien permiten la inserción de código SQL de carácter malicioso.

La inyección SQL, puede llegar de tres formas a una aplicación

- **Inband:** La información es extraída, utilizando el mismo canal que se utiliza para inyectar código SQL

- **Out-of-band:** Se utiliza un canal diferente para extraer los datos, ejemplo correo electrónico

- **Inferential:** No hay transferencia de datos, pero el atacante tiene la facultad de reconstruir la información enviando peticiones y observando el comportamiento del servidor. [72]

---

[70] BLOG.SUCURI. ¿Qué es un WAF? [En línea]. Disponible en: https://blog.sucuri.net/espanol/2018/01/que-es-un-waf.html. [Accedido Febrero 2019]
[71] SECURIZANDO. WAF-Web Application Firewall. [En línea]. Disponible en: https://securizando.com/waf-web-application-firewall/. [Accedido Febrero 2019]
[72] GUADALUPE José. Identificación y Clasificación de las Mejores Prácticas para Evitar la Inyección SQL en Aplicaciones Desarrolladas en PHP y PostgreSQL. [En línea]. Disponible en: https://cimat.repositorioinstitucional.mx/jspui/bitstream/1008/412/1/ZACTE16.pdf. [Accedido Febrero 2019]

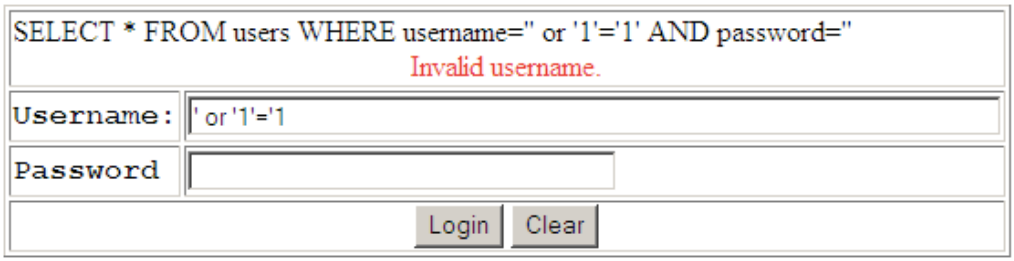
Ejemplos de Ataques por Inyección SQL

- **Uso del Operador OR**
  Sentencia vulnerable
  SELECT * FROM users WHERE username= '$username' AND password='$password'

  Ataque: Se pueden cambiar estos valores
  $username = 1' or '1' = '1
  $password = 1' or '1' = '1

  Por tanto obtenemos la siguiente consulta
  SELECT * FROM users WHERE username='1' OR '1' = '1' AND password='1' OR '1' = '1', [73] como se observa en la figura 11

  Figura 11. Ataque SQL uso del operador OR



  Fuente: MILO2012. SQL Injection for Microsoft Access, [En línea]. Disponible en https://milo2012.wordpress.com/2012/02/18/sql-injection-for-microsoft-access/. [Accedido Mayo 2020]

  Al enviar a través del get al servidor o dominio, cuando el sitio web es vulnerable, obtendremos una solicitud igual a esta
  http://www.example.com/index.php?username=1'%20or%20'1'%20=%20'1&password=1'%20or%20'1'%20=%2 0'1

  Figura 12. Ataque SQL Envío a través del get. Elaboración propia

- **Consulta SELECT**
  Sentencia Vulnerable
  SELECT * FROM Users WHERE ((Username='$username') AND (Password=MD5('$password')))

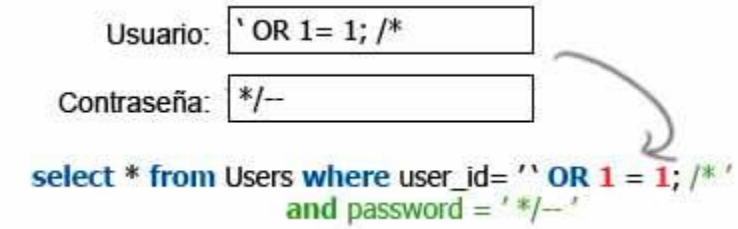
[73] Ibid, pág 15

Para el ejemplo el password utiliza la función MD5, pero en el ataque se utilizan símbolos para comentar líneas o cadenas
$username = 1' or '1' = '1'))/*
$password = foo

Para PostgreSQL y Oracle se usa el simbolo “--"

Por tanto obtenemos la siguiente consulta
SELECT * FROM Users WHERE ((Username='1' or '1' = '1'))/*') AND (Password=MD5('$password'))), [74] como se observa en la figura 13

Figura 13. Ataque SQL Consulta Select



Fuente: ESCRIBECODIGO. Ataques de Inyección SQL, [En línea]. Disponible en https://www.escribecodigo.com/ataques-de-inyeccion-de-sql/. [Accedido Mayo 2020]

El sitio quedaría así:
http://www.example.com/index.php?username=1'%20or%20'1'%20=%20'1'))/*&password=foo

Figura 14. Ataque SQL Envío a través del get Consulta Select. Elaboración propia

- **Consulta Utilizando el Operador UNION**
  Sentencia Vulnerable
  SELECT Name, Phone, Address FROM Users WHERE Id=$id

  Damos valor a id
  $id=1 UNION ALL SELECT creditCardNumber,1,1 FROM CreditCarTable
  Por tanto obtenemos la siguiente consulta

  SELECT Name, Phone, Address FROM Users WHERE Id=1 UNION ALL SELECT creditCardNumber,1,1 FROM CreditCarTable

[74] Ibid, pág 16

Esta sentencia arroja la consulta original con todos los usuarios de tarjetas de crédito [75]

- **Inyección SQL a Ciegas**
  Este método se utiliza cuando el atacante no sabe nada sobre el resultado, el caso típico es cuando el programador crea una página personalizada, que no revela la estructura de la consulta, es decir la página no devuelve un error SQL, solo devuelve un HTTP 500.

  El problema radica en que este tipo de técnica utiliza la combinación de fuerza bruta y diccionario, para buscar carácter por carácter el usuario o contraseña que contenga la base de datos atacada. [76]

Por lo anterior, es necesario contar con herramientas que permitan probar las aplicaciones web, antes de que salgan a producción, con el fin de mitigar ataques por SQL Injecction, estas pruebas consisten en “black box” y “White box”.

- **White Box:** Su finalidad es analizar el código de la aplicación sin ejecutarlo, esto se logra en base a patrones o reglas que analiza el flujo de los datos, que puede realizarse de manera manual o mediante herramientas como FORTIFY, OUNCE y PIXY entre otros, estas herramientas analizan todos los caminos posibles y cambios que se dan a través de la manipulación del código SQL, para después verificar su resultado, el éxito de estas pruebas dependerá de la complejidad, es decir que esta prueba es confiable, para estructuras pequeñas.

- **Black Box:** En una etapa temprana del desarrollo, reduce el costo de reparación por su rapidez, sin embargo tiene el problema de que puede reportar falsos positivos y negativos lo que obligaría a una revisión manual al finalizar el análisis, estos escáneres no identifican la parte interna de la estructura web, sino que lanzan pruebas sobre las peticiones http, realizando cientos y miles de pruebas de inyección SQL a través de las entradas del usuario a la espera de evaluar cuales fueron exitosos, comercialmente se encuentran herramientas como: Vuknerability Scanner, Acunetix web, Watchfire AppScan, Netsparker y libres como Brupsuite, Gamja y Grendel-Scan, sin embargo estas herramientas presentan varias limitaciones, respecto a las comerciales. [77]

Independientemente de la herramienta que se utilice, el funcionamiento de estas aplicaciones, consiste en los siguientes pasos:

[75] Ibid, pág 16
[76] Ibid, pág 17
[77] Ibid, pág 22

- **Configuración:** En esta etapa se define la URL, tecnología con la que fue creada el sitio y el tipo de prueba a realizar.

- **Exploración:** En esta etapa se reproduce un mapa de la estructura interna de la aplicación, encontrando las páginas que van a ser probadas y escaneadas.

- **Escaneo:** En esta etapa, el escaneo inicia en la página principal buscando todos los link disponibles e ingresando a cada uno de ellos para ejecutar pruebas de penetración automatizadas, simulando ser un usuario en el navegador, para encontrar todos los campos que requieran información y realizar los ataques, al finalizar esta prueba se generará un reporte con las vulnerabilidades encontradas, su clasificación (alta, media, baja) y las posibles formas para darle solución. [78]

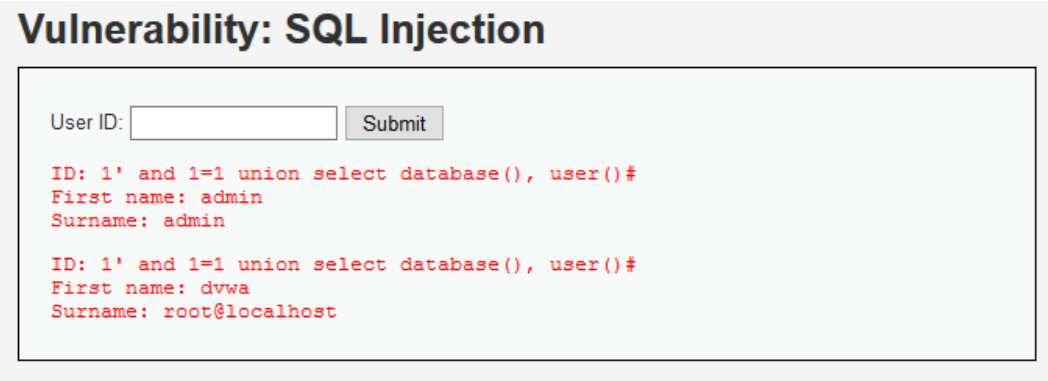
Elementos que se deben considerar en PostgreSQL

- Las sentencias en PostgreSQL son truncadas utilizando el carácter de comentario --
- LIMIT y OFFSET, son instrucciones que se utilizan la sentencia SELECT para que devuelva una parte del resultado de la consulta

Ejemplos:

Función versión(): sirve para obtener el banner PostgreSQL, además muestra el sistema operativo y su versión, la figura 15 muestra diferentes versiones de cómo utilizar el operador unión [79]

Figura 15. Ataque SQL operador Unión

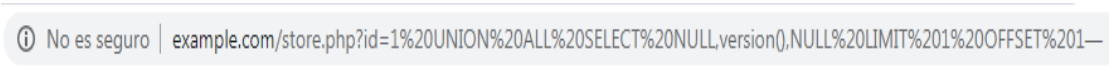


[78] Ibid, pág 23
[79] Ibid, pág 19

Fuente: SYSTEMIZES65. Hacking desde 0. Hoy SQL Injecction, [En línea]. Disponible en http://systemizes65.rssing.com/chan-58145701/latest.php. [Accedido Mayo 2020]

http://www.example.com/store.php?id=1 UNION ALL SELECT NULL,version(),NULL LIMIT 1 OFFSET 1—

Figura 16. Ataque SQL Envío a través del get Consulta Unión. Elaboración propia



Resultado
PostgreSQL 9.1.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.4-2ubuntu4) [80]

Función LENGTH(str) Devuelve la longitud de la cadena
SUBSTR(str,index,offset) Extrae parte de una cadena

Detener la comilla simple: Se recomienda codificar las cadenas, mediante el uso de la función chr(), ya que esta devuelve el valor ascci del parámetro pasado, es decir que si deseamos codificar la cadena root, debemos hacer lo siguiente:
select ascii('r')
114
select ascii('o')
111
select ascii('t')
116
Al codificar 'root' queda como:
chr(114)||chr(111)||chr(111)||chr(116)
En el navegador se vería de la siguiente forma:

http://www.example.com/store.php?id=1; UPDATE users SET PASSWORD=chr(114)||chr(111)||chr(111)||chr(116)--, [81] como se muestra en la figura 17

[80] Ibid, pág 19
[81] Ibid, pág 20

Figura 17. Ataque SQL Envío a través del get, uso de ascii. Elaboración propia

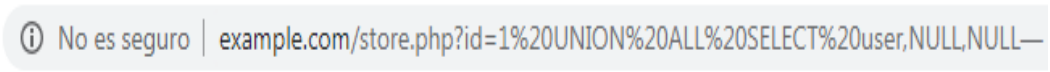
Vectores de Ataque

- Usuario Actual: Se utiliza para obtener el usuario actual, se pueden utilizar las siguientes consultas

    - SELECT user
    - SELECT current_user
    - SELECT session_user
    - SELECT usename FROM pg_user
    - SELECT getpgusername()

  Ejemplos:
  http://www.example.com/store.php?id=1 UNION ALL SELECT user,NULL,NULL— [82]

  Figura 18. Ataque SQL Envío a través del get, uso de UNION ALL. Elaboración propia

  http://www.example.com/store.php?id=1 UNION ALL SELECT current_user, NULL, NULL—

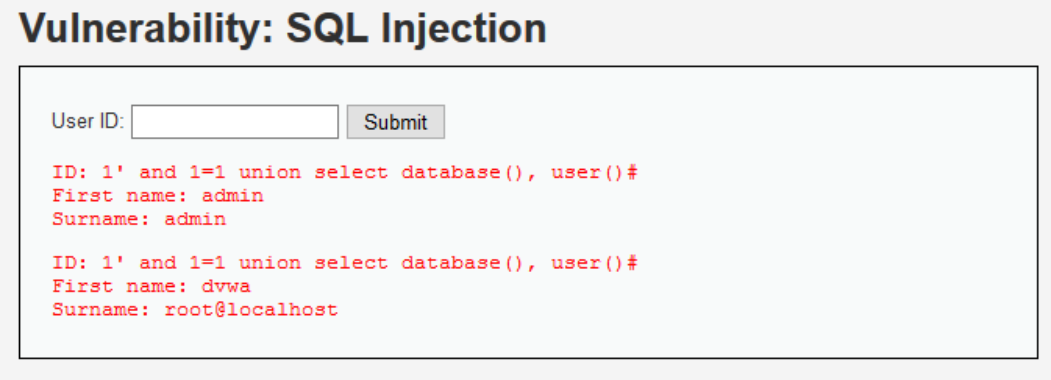
  Figura 19. Ataque SQL Envío a través del get, uso de UNION ALL. Elaboración propia

- Base de Datos Actual: La función current_database() devuelve el nombre de la base de datos, como se muestra en la figura 18

  Figura 20. Ataque SQL operador current_database()

[82] Ibid, pág 20



Fuente: SYSTEMIZES65. Hacking desde 0. Hoy SQL Injecction, [En línea]. Disponible en http://systemizes65.rssing.com/chan-58145701/latest.php. [Accedido Mayo 2020]

Ejemplo http://www.example.com/store.php?id=1 UNION ALL SELECT current_database(),NULL,NULL— [83]

Figura 21. Ataque SQL Envío a través del get, uso de UNION ALL. Elaboración propia

- Leer un Archivo: PostgreSQL tiene dos formas de acceder a un archivo
  - Sentencia COPY: Copia datos entre un archivo y una tabla
  - pg_read_file(): Permite leer archivos arbitrariamente dentro del directorio del sistema manejador de base de datos.

4.3.9 Buenas Prácticas para Evitar Inyecciones SQL

Existen diferentes medidas que contribuyen al fortalecimiento de la seguridad de la base de datos, para prevenir y mitigar ataques de este tipo, para eso debemos seguir la siguientes fases:

- **Definición y Diseño:** En esta fase se debe puntualizar los requerimientos de arquitectura y definición de permisos, para esto debemos seguir los siguientes pasos:
  - definir una arquitectura que permita separar el código de los datos

[83] Ibid, pág 21

- Seleccionar un framework que brinde protección contra ese tipo de vulnerabilidades
- Definir cuentas, solo con los privilegios estrictamente necesarios,
- Definir los permisos de acceso a la base de datos para cada cuenta
- Validar los campos de entrada (Tamaño y Tipo)

- **Desarrollo:** En esta fase se debe construir los elementos y procedimientos, que se deben utilizar, para proteger la base de datos, siguiendo las siguientes recomendaciones:
  - Utilizar consultas parametrizadas
  - Diseño apropiado de los procedimientos almacenados
  - Configurar las directivas de seguridad, de la herramienta de desarrollo
  - Realizar el ocultamiento de la información con el fin de no mostrar los errores al usuario
  - Delimitar los valores de la consulta
  - Realizar revisión de códigos, para descartar falsos positivos

- **Implementación:** Aplicar los procedimientos diseñados en la etapa anterior y reforzar con las siguientes medidas:
  - Utilizar firewall contra inyección SQL
  - Aislar la aplicación web [84]

4.3.10 Procedimiento para Prevenir Ataques por Abuso de Privilegios

Este tipo de ataque, es al que más se enfrentan las compañías, aproximadamente el 80 % de ataques corresponde a este ítem, convirtiéndose en uno de los mayores peligros que tienen que enfrentar las organizaciones, por tanto es importante realizar los siguientes controles para reducir o mitigar el riesgo de ataque por el uso excesivo de privilegios

- Contar con un registro de auditoria, para que antes de realizarse una consulta sobre la base de datos, se cree un registro de seguimiento.

- Revisar los planes de auditoria, para buscar posibles conexiones anómalas, consultas fuera de horarios laborales, eliminación y/o actualización de registros.

- Contar con herramientas diferentes al sistema manejador de base de datos, para registrar los intentos de conexiones y conexiones realizadas.

[84] Ibid, pág 35

- Analizar los valores de los parámetros enviados por el usuario a través de la aplicación, con el fin de detectar y descartar el uso de caracteres especiales, para prevenir ataques por inyección SQL.

- Realizar análisis y pruebas de vulnerabilidades al código de ejecución que realiza las consultas de la base de datos.

- Procurar por usar procedimientos almacenados, ya que esto dificulta el uso de consultas concatenadas,

4.3.11 Procedimiento para Prevenir Ataques por Uso Excesivo de Privilegios

Hace referencia a usuarios que cuentan con permisos más de los necesarios, para realizar su trabajo, esta vulnerabilidad se da al momento de crear los usuarios por parte de los BDA, al no contar con una política clara de control de accesos, los siguientes controles, permiten mitigar este riesgo:

- Contar con la política del principio de privilegios mínimo
- Crear schemas para clasificar y agrupar los objetos de la base de datos como tablas, funciones, procedimientos almacenados y vistas
- Asignar permisos mediante el uso de roles en vez de asignarse directamente a los usuarios
- Desactivar los usuarios por defecto del motor de base de datos
- Utilizar las herramientas de auditoria, para realizar oportunamente los seguimientos en la base de datos
- Monitorear los usuarios que tienen permisos de administrador sobre la base de datos. [85]

4.3.12 Procedimiento para Prevenir Ataques por Malware

Este tipo de ataques, se consideran los más elaborados, ya que su estrategia es tomar el control de equipos silenciosamente utilizando varios medios para su propagación como páginas web, correos electrónicos, ingeniería social, software pirata y memorias USB entre otros, por tanto algunas medidas para mitigar el riesgo de infección son las siguientes:

- Evitar la instalación de software pirata en servidores y equipos administrativos.

[85] UNAB. Database Main Threats Analisys, [En línea]. Disponible en: http://www.unab.edu.co/sites/default/files/MemoriasGrabadas/papers/capitulo9_paper_10.pdf. [Accedido Febrero 2019]

- Contar con las últimas actualizaciones del sistema operativo en el servidor y motor base de datos.

- Instalar y configurar correctamente herramientas firewall tanto físicas como lógicas con las debidas reglas de acceso.

- Restringir el acceso a la base de datos, para evitar conexiones utilizando internet, redes externas, conexiones inalámbricas.

- Realizar una correcta asignación de roles y/o permisos a los usuarios, con el fin de evitar otorgar permisos de súper usuario o administrador a usuarios que no deben contar con ese tipo de acceso

4.3.13 Procedimiento para Prevenir Ataques por Vulnerabilidades de Base de Datos no Configuradas

Es muy común encontrarse con motores de bases de datos y sistemas operativos sin actualizaciones, instalaciones con usuarios por defecto y sin seguridad, bases de datos que fueron restauradas en entornos de prueba, sin la debida protección, servidores de base de datos con acceso a internet, servidores web compartiendo instalación con los servidores de base de datos y usuarios con excesivos privilegios que le permitirán a usuarios externos o internos, tomar el control de la base de datos, por tanto las siguientes recomendaciones, ayudaran a mitigar los riesgos, para que se lleven a cabo este tipo de ataques:

- Se debe contar con un plan de actualizaciones a nivel de sistema operativo y motor de base de datos, que permita contar con las últimas actualizaciones, teniendo especial cuidado de aplicarlas en un ambiente de pruebas, antes de llevarlas a producción.

- Utilizar cuentas de inicio de sesión, que correspondan a un dominio y utilizando la política del nivel de privilegios mínimo.

- No utilizar las cuentas propias del sistema operativo, para iniciar los servicios del motor de base de datos, ya que son cuentas con un nivel elevado de privilegios.

- No instalar el servidor web en el mismo lugar del servidor de base de datos.

- Cifrar la comunicación del canal de datos con el servidor de base de datos.

- Evitar el acceso al servidor de base de datos, desde una red externa, además la red interna debe contar con firewall, que permita crear reglas de acceso.

- Identificar los peligros potenciales dentro de la organización, que involucre el servidor de base de datos, para que realice constante monitoreo

4.3.14 Procedimiento de Configuración Inicial de una Base de Datos PostgreSQL.

A continuación describiré como realizar la configuración inicial de PostgreSQL 11, para evitar ataques por base de datos no configuradas, partiendo de que la instalación se llevó a cabo en un servidor con sistema operativo Linux CentOs 7

- **Configuración:** En esta etapa se deben encontrar los archivos de configuración luego de su instalación, para esto abrimos una terminal y escribimos la siguiente instrucción find / -name postgresql* tal como se muestra en la figura 22

Figura 22. Búsqueda de Archivos de Configuración de PostgreSQL

```
find / -name postgresql*
```

Fuente: DAIGOR. Instalación y Configuración Inicial de PostgreSQL-11, [En línea]. Disponible en https://daigor.dev/post/postgres11-conf-init/. [Accedido Mayo 2020]

A continuación se debe iniciar la instancia de PostgreSQL, con la siguiente instrucción /usr/pgsql-11/bin/postgresql-11setup initdb, como se muestra en figura 23

Figura 23. Inicializar la Base de Datos PostgreSQL

```
/usr/pgsql-11/bin/postgresql-11-setup initdb
```

Fuente: DAIGOR. Instalación y Configuración Inicial de PostgreSQL-11, [En línea]. Disponible en https://daigor.dev/post/postgres11-conf-init/. [Accedido Mayo 2020]

El paso anterior creara en el sistema el directorio y los archivos de configuración inicial, aquí se debe utilizar el usuario postgres, para encontrar la ruta de datos de PostgreSQL, como se muestra en la figura 24

Figura 24. Cambio a Usuario PostgreSQL y Ruta de Datos

```
# Cambiamos al usuario 'postgres'

su - postgres

# Encontramos la ruta de datos de PostgreSQL

find / -name pg-hba.conf 2>/dev/null
```

/var/lib/pgsql/11/data/pg_hba.conf

Fuente: DAIGOR. Instalación y Configuración Inicial de PostgreSQL-11, [En línea]. Disponible en https://daigor.dev/post/postgres11-conf-init/. [Accedido Mayo 2020]

Ahora se debe editar el archivo de configuración .bash_profile, para agregar la variable PGDATA, como se muestra en la figura 25

Figura 25. Edición del Archivo .bash_profile

```
cd ~
vim .bash_profile
```

Fuente: DAIGOR. Instalación y Configuración Inicial de PostgreSQL-11, [En línea]. Disponible en https://daigor.dev/post/postgres11-conf-init/. [Accedido Mayo 2020]

Agregando la línea export PGDATA=/var/lib/pgsql/11/data/, como se muestra en la figura 26

Figura 26. Línea Export PGDATA

```
export PGDATA=/var/lib/pgsql/11/data/
```

Fuente: DAIGOR. Instalación y Configuración Inicial de PostgreSQL-11, [En línea]. Disponible en https://daigor.dev/post/postgres11-conf-init/. [Accedido Mayo 2020]

A continuación encontrar la ruta de los binarios, como se muestra en la figura 27

Figura 27. Búsqueda Archivos Binarios PostgreSQL

```
find / -name pg_ctl 2>/dev/null
```

/usr/pgsql-11/bin/pg_ctl

Fuente: DAIGOR. Instalación y Configuración Inicial de PostgreSQL-11, [En línea]. Disponible en https://daigor.dev/post/postgres11-conf-init/. [Accedido Mayo 2020]

Editar el archivo .bash_profile para agregar al PATH la ruta de los binarios de PostgreSQL, como se muestra en la figura 28

Figura 28. Concatenación a la Variable PATH de la Ruta de los Binarios

```
PATH=$PATH:$HOME/.local/bin:$HOME/bin:/usr/pgsql-11/bin/
export PATH
```

Fuente: DAIGOR. Instalación y Configuración Inicial de PostgreSQL-11, [En línea]. Disponible en https://daigor.dev/post/postgres11-conf-init/. [Accedido Mayo 2020]

- **Comprobación:** En esta etapa se verifica si la terminal interactiva de PostgreSQL funciona, para esto se debe iniciar el servicio del servidor, como se muestra en la figura 29

Figura 29. Inicio del Servicio PostgreSQL

```
pg_ctl start
```

Fuente: DAIGOR. Instalación y Configuración Inicial de PostgreSQL-11, [En línea]. Disponible en https://daigor.dev/post/postgres11-conf-init/. [Accedido Mayo 2020]

Si todo se ha configurado correctamente, deberá aparecer en la terminal psql, como se muestra en la figura 30

Figura 30. Terminal Interactiva de PostgreSQL

```
psql
```

Fuente: DAIGOR. Instalación y Configuración Inicial de PostgreSQL-11, [En línea]. Disponible en https://daigor.dev/post/postgres11-conf-init/. [Accedido Mayo 2020]

- **Firewall:** Con el fin de establecer una conexión remota que permita la administración, sin necesidad de ir directamente al servidor, se debe añadir una regla de configuración al firewall, para esto verificamos las solicitudes de conexión que el servidor acepta, se debe tener en cuenta que PostgreSQL acepta conexiones remotas por medio del puerto 5432, en CentOS se utiliza la instrucción firewall-cmd –list-all para ver las conexiones permitidas, como se muestra en la figura 31

Figura 31. Lista de Conexiones Aceptadas por el Firewall

```
firewall-cmd --list-all
```

```
...
ports: 8081/tcp
...
```

Fuente: DAIGOR. Instalación y Configuración Inicial de PostgreSQL-11, [En línea]. Disponible en https://daigor.dev/post/postgres11-conf-init/. [Accedido Mayo 2020]

Se Agrega la regla nueva regla que permita acceder al servicio 5432, como se muestra en la figura 32

Figura 32. Configuración de Regla en el Firewall para Acceso al Puerto 5432

```
firewall-cmd --add-port 5432/tcp --permanent
```

Fuente: DAIGOR. Instalación y Configuración Inicial de PostgreSQL-11, [En línea]. Disponible en https://daigor.dev/post/postgres11-conf-init/. [Accedido Mayo 2020]

Ahora se recarga la configuración del firewall y se lista las reglas, para verificar que la configuración está correcta, como se muestra en la figura 33

Figura 33. Comprobación de las Reglas del Firewall en CentOs 7

```
# Recargamos la configuración del firewall

firewall-cmd --reload

# Listamos la configuración para verificar que se agrego correctamente

firewall-cmd --list-all
```

```
...
ports: 8081/tcp 5432/tcp
...
```

Fuente: DAIGOR. Instalación y Configuración Inicial de PostgreSQL-11, [En línea]. Disponible en https://daigor.dev/post/postgres11-conf-init/. [Accedido Mayo 2020]

- **Conexión:** Ahora se le debe decir al servidor PostgreSQL, que puerto y desde que direcciones puede atender conexiones, para esto se ingresa a la terminal interactiva, se cambia al usuario postgres, luego se buscar el directorio de datos y se edita el archivo postgresql.conf como se muestra en la figura 34

Figura 34. Edición del Archivo postgresql.conf

```
# Cambiamos a usuario 'postgres'

su - postgres

# Entramos al directorio de datos de PostgreSQL

echo $PGDATA

# Editamos el archivo postgresql.conf

vim postgresql.conf

# Buscamos la sección '# CONNECTIONS AND AUTHENTICATION'
```

Fuente: DAIGOR. Instalación y Configuración Inicial de PostgreSQL-11, [En línea]. Disponible en https://daigor.dev/post/postgres11-conf-init/. [Accedido Mayo 2020]

Ahora se descomenta la línea #port = 5432 y se agrega la expresión regular *, en caso de querer que cualquier IP se conecte a la base de datos, como se muestra en la figura 35

Figura 35. Conexión y Autenticación

```
#port = 5432

port = 5432
```

```
#listen_addresses = 'localhost'

listen_addresses = '*'
```

Fuente: DAIGOR. Instalación y Configuración Inicial de PostgreSQL-11, [En línea]. Disponible en https://daigor.dev/post/postgres11-conf-init/. [Accedido Mayo 2020]

- **Autenticación:** Tras haber configurado la conexión remota, ahora es necesario controlar los siguientes aspectos:
    - A quien se le permite el acceso
    - Con cual método de autenticación
    - Que usuarios de PostgreSQL pueden ingresar
    - A cuales bases de datos pueden acceder

Esta configuración se debe definir en el archivo pg_hda.conf, el cual se encuentra en el directorio de datos de PostgreSQL PGDATA, como se muestra en la figura 36

Figura 36. Edición del Archivo pg_hda.conf

```
# Entramos al directorio de datos de PostgreSQL

echo $PGDATA

# Editamos el archivo postgresql.conf

vim pg_hda.conf
```

Fuente: DAIGOR. Instalación y Configuración Inicial de PostgreSQL-11, [En línea]. Disponible en https://daigor.dev/post/postgres11-conf-init/. [Accedido Mayo 2020]

Aquí se debe cambiar el método de autenticación de trust a md5, como se muestra en la figura 37

Figura 37. Cambio de Método de Autenticación

```
# TYPE  DATABASE        USER            ADDRESS                 METHOD

local   all             all                                     trust

# TYPE  DATABASE        USER            ADDRESS                 METHOD

local   all             all                                     md5
```

Fuente: DAIGOR. Instalación y Configuración Inicial de PostgreSQL-11, [En línea]. Disponible en https://daigor.dev/post/postgres11-conf-init/. [Accedido Mayo 2020]
Se debe agregar un registro nuevo, con el fin de que cualquier usuario se pueda conectar a la base de datos de prueba, que se creará más adelante y únicamente se podrá acceder a través de la dirección IP 10.20.0.0/16, como se muestra en la figura 38

Figura 38. Conexión de Prueba

```
# Prueba

host    prueba      all     10.20.0.0/16        md5
```

Fuente: DAIGOR. Instalación y Configuración Inicial de PostgreSQL-11, [En línea]. Disponible en https://daigor.dev/post/postgres11-conf-init/. [Accedido Mayo 2020]

Para que los cambios tengan efecto se debe recargar el servicio de PostgreSQL, utilizando la instrucción pg_ctl reload, como se muestra en la figura 39

Figura 39. Recargar el Servicio de PostgreSQL

```
pg_ctl reload
```

Fuente: DAIGOR. Instalación y Configuración Inicial de PostgreSQL-11, [En línea]. Disponible en https://daigor.dev/post/postgres11-conf-init/. [Accedido Mayo 2020]

- **Usuarios:** Una de las buenas prácticas es cambiar la contraseña del superusuario postgres, ya que este usuario tiene todos los permisos de administración de la base de datos, en lo posible este usuario no debe utilizarse para labores cotidianas, para esto accedemos a la terminal interactiva, y se realiza el cambio de contraseña, como se muestra en la figura 40

Figura 40. Cambio de Contraseña de un Usuario

```
-- Cambiamos la contraseña

postgres=# alter user postgres with password '[password]';
```

Fuente: DAIGOR. Instalación y Configuración Inicial de PostgreSQL-11, [En línea]. Disponible en https://daigor.dev/post/postgres11-conf-init/. [Accedido Mayo 2020]

Ahora se crea una base de datos de prueba como se muestra en la figura 41

Figura 41. Creación de una Base de Datos

```
-- Creamos la base de datos 'prueba'

postgres=# create database prueba;

-- Creamos un nuevo usuario

postgres=# create user [user_name] with password '[password]';
```

Fuente: DAIGOR. Instalación y Configuración Inicial de PostgreSQL-11, [En línea]. Disponible en https://daigor.dev/post/postgres11-conf-init/. [Accedido Mayo 2020]

Los campos [user_name] y '[password]' se deben reemplazar con los datos del nuevo usuario, ahora al nuevo usuario se le debe volver propietario de la base de datos prueba, como se muestra en la figura 42

Figura 42. Volver Propietario al Nuevo Usuario de la BD Prueba

```
-- Al nuevo usuario lo volvemos propietario de la base de datos 'prueba'

postgres=# alter database prueba owner to [user_name];

-- Salimos

postgres=# q
```

Fuente: DAIGOR. Instalación y Configuración Inicial de PostgreSQL-11, [En línea]. Disponible en https://daigor.dev/post/postgres11-conf-init/. [Accedido Mayo 2020]

Recargar el servicio, para aplicar los cambios.

- **Conexión Remota:** Para establecer una conexión remota desde un cliente, es necesario que este tenga instalado el cliente de PostgreSQL, para

realizar la conexión es necesario conocer la dirección IP del servidor y ejecutar la instrucción psql –h [dir_ip] –d [base_datos] –u [user_name], como se muestra en la figura 43

Figura 43. Conexión Remota

```
psql -h [ip_address] -d [database_name] -U [user_name]
```

Fuente: DAIGOR. Instalación y Configuración Inicial de PostgreSQL-11, [En línea]. Disponible en https://daigor.dev/post/postgres11-conf-init/. [Accedido Mayo 2020]

Ip_address se reemplaza por la dirección ip del servidor, database_name el nombre de la base de datos y user_name el nombre del usuario.
Por último se debe comprobar que el usuario creado es el propietario de la base de datos de prueba, esto se logra creando y eliminando una tabla [86] como se muestra en la figura 44

Figura 44. Crear y Eliminar Tabla

```
prueba=> CREATE TABLE tabla_test();
```

CREATE TABLE

```
prueba=> DROP TABLE tabla_test;
```

DROP TABLE

Fuente: DAIGOR. Instalación y Configuración Inicial de PostgreSQL-11, [En línea]. Disponible en https://daigor.dev/post/postgres11-conf-init/. [Accedido Mayo 2020]

[86] DAIGOR. Instalación y Configuración Inicial de PostgreSQL-11, [En línea]. Disponible en https://daigor.dev/post/postgres11-conf-init/ [Accedido Mayo 2020]

4.3.15 Metodología para Prevenir Intrusiones a las Bases de Datos PostgreSQL

Para abordar el problema y dar una solución que mitigue el riesgo de intrusión a las bases de datos PostgreSQL, es necesario que dicho planteamiento se base en el ciclo de mejora continua PHVA.

Figura 45. Ciclo PHVA

Fuente: AULAFACIL. El ciclo PHVA, [En línea]. Disponible en: https://www.aulafacil.com/cursos/administracion/gestion-de-la-calidad/el-ciclo-phva-l35719. [Accedido Abril 2019]

Este planteamiento se debe a que la tecnología no para de avanzar, por tanto hay que ser consciente que día a día el poder de procesamiento aumenta, se desarrollan nuevas herramientas para proteger y atacar en la red, por tanto, cualquier metodología deba plantearse como un ciclo de mejora continua.

- **Planear**

  En esta etapa debemos considerar los siguientes elementos
  - **Identificación**: En este paso se deben analizar las aplicaciones que requieren ser protegidas, estas aplicaciones comprenden el sistema gestor de base de datos, sistemas operativos y aplicaciones que se conectan a la base de datos, como se muestra en la tabla

Tabla 2. Inventario de Software. Elaboración Propia

SOFTWARE	NOMBRE	VERSIÓN
Sistema Operativo	Linux CentOS	7
Motor de Base de Datos	PostgreSQL 11	11
Aplicativo Web	Aplicativo de Prueba	1

- **Recopilación**: Se debe recopilar toda la documentación con que se cuenta, acerca de la configuración del motor de base de datos, sistema operativo que aloja el motor de base de datos, diccionario, manual de desarrollo y manual del usuario de las aplicaciones que se conectan a la base de datos postgresql de la organización, adicional a esto es necesario contar con la documentación del lenguaje de programación, con el que se desarrollaron dichas aplicaciones.

- **Definir los Parámetros a Mejorar**: En este paso se debe establecer, cuáles son los parámetros que se deben mejorar, producto de la identificación y la recopilación de la documentación realizada en las etapas anteriores, igualmente se debe hacer un análisis para verificar el cumplimiento de seguridad del sistema gestor de base de datos, de acuerdo a los procedimientos establecidos para evitar o mitigar ataques por los diferentes métodos analizados en los numerales anteriores.

- **Hacer**

  En esta etapa se deben realizar los siguientes pasos:
  - **Test de Vulnerabilidades**: Para la realización de estas pruebas de vulnerabilidades, se utilizan herramientas, que realicen un proceso automático de verificación como NMAP, SQLMAP, NESSUS, PIPPER, BSQL HACKER entre otras, las cuales las podemos encontrar en suites como OWASP y KALI Linux y seguir estos pasos:

    - **Buscar Vulnerabilidades**: Aquí se debe realizar de manera manual, la búsqueda de las diferentes vulnerabilidades, utilizando las herramientas descritas anteriormente, para clasificarlas en vulnerabilidades de sistema operativo, sistema gestor de base de datos y aplicaciones.

    - **Test de Intrusión**: la información obtenida en el punto anterior, nos sirve para consultarla en el sitio https://cve.mitre.org/, el cual se encarga de clasificar y publicar, todos los reportes de fallos de seguridad, encontrados y/o reportados por los distintos fabricantes

de software, el cual brinda información necesaria, para realizar un intento de adquirir permisos o permitir modificaciones sobre la base de datos, al igual que ingresar a un equipo, por medio de fallos del sistema operativo u otras aplicaciones instaladas.
El OWASP ASVS (estándar de verificación de aplicación de seguridad) tiene definido un grupo de áreas, que deben ser evaluadas y cada una de estas áreas, tienen un grupo de requerimientos que deben cubrir, estas áreas son: [87]

V1: Arquitectura, diseño y modelado de amenazas
Este objetivo de control busca que la aplicación auditada cumpla los siguientes requisitos:

- Nivel 1, Los componentes de la aplicación son identificables y tienen una razón de existir.

- Nivel 2, Cuenta con una arquitectura definida y el código es consistente con ésta.

- Nivel 3, La arquitectura y el diseño son los adecuados (son eficaces). [88]

V2: Requisitos de verificación de autenticación
Teniendo en cuenta que la autenticación es el acto de confirmar o establecer alguien o algo como verdadero o auténtico, se debe verificar que la aplicación cumple con los siguientes requisitos:

- Verificación digital de la identidad del remitente, en una comunicación.

- Asegurar que sólo usuarios que están autorizados, tienen la capacidad de autenticarse y que las credenciales se transporten de forma segura. [89]

V3: Requisitos de verificación de gestión de sesiones
El componente básico de cualquier aplicación web, es el método que controla y mantiene el estado del usuario al momento de interactuar con ésta, llamada manejo de sesiones, por tanto la aplicación debe satisfacer los siguientes requisitos:

---

[87] OWASP. Estándar de verificación de seguridad en aplicaciones, [En línea]. Disponible en: https://www.owasp.org/images/6/67/OWASPApplicationSecurityVerificationStandard3.0.pdf. [Accedido Abril 2019]
[88] Ibid, pág 23
[89] Ibid, pág 25

- Las sesiones son únicas para cada usuario o individuo, jamás compartidas.
- Las sesiones se deben invalidar, cuando ya no son necesarias o se han sobrepasado los límites de tiempo de inactividad. [90]

V4: Requisitos de verificación del control de acceso
La autorización es la facultad de permitir el acceso únicamente a los usuarios que se les ha permitido su utilización, por tanto, se debe verificar que la aplicación cumpla los siguientes requisitos:

- Los usuarios que acceden a los recursos, cuentan con credenciales válidas para realizarlo.

- Los usuarios se encuentran vinculados con un conjunto estrictamente definido de roles y privilegios.

- Los metadatos de los permisos roles, se encuentran protegidos de ataques de manipulación o reutilización. [91]

V5: Requisitos de verificación para manejo de entrada de datos maliciosos
Se debe asegurar, que todas las entradas que puedan ser modificadas, estén perfectamente validadas, realizando un chequeo de la longitud de dichas entradas, para que no permita un número mayor de caracteres al que puede recibir la entrada, igualmente se debe restringir el uso de caracteres especiales que puedan modificar el código de la base de datos, es recomendable realizar esta labor al lado del servidor, para evitar ataques cross site scripting, inyección SQL, desbordamiento de búfer entre otros, así mismo se debe examinar que no existan puertas traseras, por donde un atacante pueda infiltrarse, por tanto se debe verificar que la aplicación cumple los siguientes requisitos:

- Todas las entradas están validadas correctamente y definidas para su propósito.

- No se debe confiar en datos de una entidad cliente o externa, deben tratarse como tales. [92]

V6: Codificación / escape de salida de datos
Esta sección se incorporó en el anterior ítem V5. [93]

[90] Ibid, pág 29
[91] Ibid, pág 31
[92] Ibid, pág 33

V7: Requisitos de verificación para la criptografía en el almacenamiento

Se debe verificar que la aplicación satisface los siguientes requisitos:

- Que todos los módulos criptográficos fallen de forma segura y que estos errores se gestionen correctamente.
- Que se utilice un generador aleatorio de números, cuando se requiera la aleatoriedad.
- Que el acceso a claves se realice de forma segura. [94]

V8: Requisitos de verificación de gestión y registro de errores

Su objetivo es crear registros de alta calidad con información útil para administradores, usuarios, y equipos de respuesta a incidentes, por tanto se debe verificar que la aplicación cumpla los siguientes requisitos:

- No registrar la información considerada confidencial si no se requiere.
- Garantizar que los datos que se registran, se almacenen de forma segura y protegida según la clasificación de los datos.
- Asegurar que los datos de bitácora no se almacenen indefinidamente, sino que posean un ciclo de vida útil y corto [95]

V9: Requisitos de verificación de protección de datos

La aplicación tiene la responsabilidad de que los datos almacenados en los diferentes dispositivos, se encuentren cifrados y no puedan ser obtenidos, divulgados o alterados, por tanto se debe verificar que la aplicación cumpla los siguientes requisitos:

- Confidencialidad: Los datos deben ser protegidos de su observación no autorizada o que sean divulgados cuando se encuentran en tránsito o almacenados.
- Integridad: Los datos deben ser protegidos para que no sean alterados o eliminados por intrusos o personas no autorizadas.

---

[93] Ibid, pág 37
[94] Ibid, pág 38
[95] Ibid, pág 40

- Disponibilidad: Los datos deben estar disponibles para su uso o consulta por parte de los usuarios autorizados, cuando se requiera. [96]

V10: Requisitos de verificación de seguridad de las comunicaciones
Se debe verificar que la aplicación cumple con los siguientes requisitos:

- Utilización de TLS donde transite información sensible

- Utilización de algoritmos y cifradores fuertes siempre. [97]

V11: Requisitos de verificación de configuración de seguridad HTTP
Se debe verificar que la aplicación cumple con los siguientes requisitos:

- El servidor de aplicaciones, cuenta con una configuración endurecida preestablecida.

- Todas las respuestas HTTP tienen su tipo de contenido establecido, con un conjunto de caracteres seguro. [98]

V12: Requisitos de verificación de configuración de seguridad
Esta sección se incorporó en el anterior ítem V11 [99]

V13: Requisitos de verificación para controles malicioso
Se debe verificar que la aplicación cumple con los siguientes requisitos:

- La actividad maliciosa, debe ser manejada adecuadamente con seguridad, para no afectar el resto de la aplicación.

- No tiene bombas de tiempo u otros ataques basados en tiempo.
- No realiza “phone home” a destinos no autorizados o malintencionados.

[96] Ibid, pág 42
[97] Ibid, pág 45
[98] Ibid, pág 48
[99] Ibid, pág 50

- La aplicación no tiene puertas traseras, ataques huevos de pascua, salami, o fallos de lógica que puedan ser utilizados por un atacante. [100]

V14: Requisitos de verificación de seguridad interna
Esta sección se incorporó en el anterior ítem V13 [101]

V15: Requisitos de verificación para lógica de negocios
Se debe verificar que la aplicación cumple con los siguientes requisitos:

- El aplicativo cuenta con un flujo de lógica del negocio secuencial y en orden.

- La lógica tiene límites para evitar y detectar ataques automatizados, como transferencia de fondos pequeños agregando 1 millón de amigos.

- La lógica posee protección contra alteración, falsificación repudio, ataques de elevación de privilegios y revelación de información [102]

V16: Requisitos de verificación de archivos y recursos
Se debe verificar que la aplicación cumple con los siguientes requisitos:

- Los datos considerados como no confiables deben tratarse como tal y gestionados de forma segura.

- Los datos obtenidos de fuentes no confiables, deben ser almacenados fuera del webroot con permisos limitados. [103]

V17: Requisitos de verificación móvil
Las aplicaciones móviles deben:

- Contar con el mismo nivel de controles de seguridad, tanto en el servidor como en el cliente móvil, utilizando controles de seguridad, en un ambiente de confianza.

[100] Ibid, pág 51
[101] Ibid, pág 52
[102] Ibid, pág 53
[103] Ibid, pág 54

- Los activos de información sensibles, que se encuentren almacenados en el dispositivo, se deben realizar de forma segura.
- Se debe asegurar la capa transporte con el fin de transmitir de forma segura los datos sensibles. [104]

V18: Requisitos de verificación de servicios web
Asegurarse que en caso que la aplicación utilice los servicios web REST o SOAT, posea:

- Autenticación, gestión de sesión y autorización para todos los servicios web.

- Validación de los datos de entrada, para los parámetros que transitan en zonas de menor a mayor confianza.

- Interoperabilidad para la capa de servicios web SOAP, para el uso de la API. [105]

V19: Requisitos de configuración
La aplicación verificada debe:

- Utilizar plataformas y bibliotecas actualizadas.

- Contar con una configuración segura por omisión.

- Contar con un hardening suficiente para que los cambios realizados por un usuario, no terminen en exponer innecesariamente la información o se creen fallos de seguridad a los sistemas subyacentes. [106]

- **Evaluación del Riesgo**: En este paso se clasifica cada uno de los riesgos que se obtuvieron en el paso anterior, teniendo en cuenta que a pesar de que se han planteado muchas soluciones a los problemas presentes en la seguridad de la información, se aprecia que la inseguridad es latente en los sistemas de información y que aún no se ha resuelto por completo, esto debido a que los atacantes ya no quieren solo ser reconocidos o hacerse notar, sino que muchos desean lucrarse con dicha actividad, para nadie es un secreto la aparición de nuevas amenazas y ataques dirigidos a objetivos específicos.

[104] Ibid, pág 56
[105] Ibid, pág 58
[106] Ibid, pág 60

Por todo esto, las organizaciones deben tener presente que los riesgos tienen dos orígenes:

a) Surgimiento y evolución de nuevas amenazas.

b) Adopción de nuevas tecnologías que originan riesgos imprevistos.

Algo que las organizaciones no pueden eliminar de su entorno, por tal razón reconocer y controlar la probabilidad de ocurrencia de los riesgos, minimiza el impacto que puede surgir de la materialización de los mismos.

- **Gestionar el Riesgo**: Las acciones que se toman para disminuir la ocurrencia del riesgo, se llaman controles de seguridad, que se encuentran clasificados en tres categorías:

  a) Controles físicos:
  Son las medidas tendientes a detener o prevenir el acceso no autorizado en una estructura.
  - Acceso a instalaciones solo a personal autorizado
  - Servidores críticos en lugares seguros bajo llave
  - Respaldos guardados en sitios seguros

  b) Controles lógicos o técnicos
  Son las medidas tendientes a proteger la información mediante el uso de programas informáticos
  - Endurecimiento de servidores
  - Antivirus
  - Firewalls
  - Sistemas de detección de intrusos

  c) Controles administrativos
  Son las medidas tendientes a evaluar y recuperar la información en caso de perdidas
  - Políticas y procedimientos
  - Plan de contingencia y recuperación
  - Reportes de auditorías de seguridad [107]

[107] TIPTON Harold, KRAUSE Micki. Information security management handbook, 5th. 2006

- **Verificar**

  En esta etapa se debe documentar lo realizado en la etapa anterior, con el fin de comparar los resultados, con los objetivos trazados en la etapa de planeación, que permitirán detectar que ataques, se registraron en el periodo evaluado, de que tipo y las consecuencias derivas de la intrusión registrada, para que se plantee el plan de mejora.

- **Actuar**

  Con base en la documentación anterior, realizar un análisis con el fin de determinar una de las tres posiciones que se relacionan a continuación:
  - Determinar si los controles que se hicieron son satisfactorios y no es necesario realizar el ciclo nuevamente.

  - Determinar si los controles que se hicieron no son satisfactorios y no se cumplieron las metas trazadas por tanto se debe realizar nuevamente el ciclo de mejora continua.

  - Plantear la pregunta de cómo se podría mejorar la seguridad y documentar todo el proceso. [108]

[108] GÓMEZ Iván, Diseño de metodología para verificar la seguridad en aplicaciones web contra inyecciones SQL, [En línea]. Disponible en: https://repository.unimilitar.edu.co/bitstream/handle/10654/7212/GomezGonzalezIvanCamilo2012.pdf?sequence=2&isAllowed=y [Accedido Abril 2019]

CONCLUSIONES

- Al analizar el reporte de vulnerabilidades para PostgreSQL 9.x, se concluye que esta versión presentaba profundas fallas de seguridad que le permitían a un intruso, realizar ataques SQL Injecction, obtener privilegios y provocar denegación de servicio.

- El fabricante PostgreSQL realizó el lanzamiento de 7 versiones menores de la familia 9x comprendidas por la 9.0.23, 9.1.24, 9.2.24, 9.3.25, 9.4.26, 9.5.21 y 9.6.17, esta última fue el fin de las versiones 9.x ya que a partir de la 10, se cambió el esquema a un formato “xy”, que significa que la siguiente versión menor sería 10.1 y la próxima principal sería la 11.

- Aproximadamente el 80% de los ataques que se presentan en las organizaciones, corresponde al uso excesivo de privilegios, convirtiéndose este, en el mayor peligro que debe afrontar y mitigar el profesional de la seguridad informática, para salvaguardar la información.

- La tarea de prevenir intrusiones a la base de datos, es un entorno cambiante e impredecible donde la mitigación, debe estar diseñada bajo el ciclo PHVA, el cual es un sistema que le permite al profesional de la seguridad informática, aplicar los procedimientos planteados y realizar la auditoria del mismo que le permite la mejora continua de la seguridad de la información.

BIBLIOGRAFÍA

SECURELIST. Desarrollo de las amenazas informáticas en el primer trimestre de 2018, [En línea]. Disponible en https://securelist.lat/it-threat-evolution-q1-2018-statistics/86929/

VILLALOBOS Johnny. Vulnerabilidades de Sistemas Gestores de Base de Datos, [En línea]. Disponible en: https://www.redalyc.org/html/4759/475948929016/

AMÉRICA-RETAIL. Colombia: el comercio electrónico y su potencial en el país, [En línea]. Disponible en: https://www.america-retail.com/colombia/colombia-el-comercio-electronico-y-su-potencial-en-el-pais/

CVE-2015-3165. Vulnerabilidad 2015-3165, [En línea]. Disponible en: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3165 .

BLOG.UTP. Seguridad y protección de los sistemas operativos, [En línea]. Disponible en: http://blog.utp.edu.co/seguridadso/ .

CERTSUPERIOR S DE RL DE CV. Seguridad en redes, [En línea]. Disponible en: https://www.certsuperior.com/SeguridadenRedes.aspx .

CLAVADETSCHER Charles. Autorización en PostgreSQL, 2015. [En línea]. Disponible en: http://www.schmiedewerkstatt.ch/documents/04-publications/autorizacion_en_postgresql_script_pdfa.pdf .

EMC2NET. PostgreSQL y el uso de SSL, [En línea]. Disponible en: https://e-mc2.net/es/postgresql-y-el-uso-de-ssl .

TENER Simón, PEQUEÑO Nelson. Respaldo y recuperación de datos. 2000, [En línea]. Disponible en: https://es.slideshare.net/asaelito/respaldo-y-recuperacion-de-informacion .

2NDQUADRANT. Actualizar PostgreSQL, [En línea]. Disponible en: https://www.2ndquadrant.com/es/servicios/actualizar-postgresql/ .

EL CONGRESO DE COLOMBIA. Ley 1273 de 2009, [En línea]. Disponible en: http://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf .

UNISDR.ORG. ¿Qué significa vulnerabilidad?, [En línea]. Disponible en: https://www.unisdr.org/2004/campaign/booklet-spa/page8-spa.pdf.

PLATZI. ¿Qué es PostgreSQL y cuáles son sus ventajas?, [En línea]. Disponible en: https://platzi.com/blog/que-es-postgresql/ .

EPN. Riesgo, Amenaza y Vulnerabilidad, [En línea]. Disponible en: http://epn.gov.co/elearning/distinguidos/SEGURIDAD/13_riesgo_amenaza_y_vulnerabilidad.html

Universidad Nacional de Luján. Amenazas a la seguridad de la información, [En línea]. Disponible en: http://www.seguridadinformatica.unlu.edu.ar/?q=node/12 .

ECURED. Bases de Datos, [En línea]. Dsiponible en: https://www.ecured.cu/Bases_de_datos .

SEARCHDATACENTER. Networking, redes, cableado.. similitudes y diferencias, [En línea]. Disponible en: https://searchdatacenter.techtarget.com/es/consejo/Networking-redes-cableado-similitudes-y-diferencias .

TECNOLOGÍA-INFORMÁTICA. ¿Qué es un router?, [En línea]. Disponible en: https://tecnologia-informatica.com/que-es-router-wifi-comprar-ampliar-alcance/ .

LATAM-KASPERSKY. ¿Qué es un firewall?, [En línea]. Disponible en: https://latam.kaspersky.com/resource-center/definitions/firewall .

SOFTWAREDOIT. Definición términos de software, [En línea]. Disponible en: https://www.softwaredoit.es/definicion/index.html .

VIX. ¿Qué es un hacker?, [En línea]. Disponible en: https://www.vix.com/es/btg/tech/13182/que-es-un-hacker .

CONSULTHINK.IT. ¿Qué es y en qué consiste un ataque informático?, [En línea]. Disponible en: https://consulthink.it/es/que-es-y-en-que-consiste-un-ataque-informatico/ .

ONA SYSTEMS. Vulnerabilidades importantes que afectan la seguridad de bases de datos en las empresas, [En línea]. Disponible en: https://www.onasystems.net/vulnerabilidades-importantes-afectan-la-seguridad-bases-datos-las-empresas/ .

AVAST. Malware & Antimalwalre, [En línea]. Disponible en: https://www.avast.com/es-es/c-malware .

INFOSPYWARE. ¿Qué son los virus informáticos?, [En línea]. Disponible en: https://www.infospyware.com/articulos/%C2%BFque-son-los-virus-informaticos/ .

KASPERSKY. Gusanos informáticos, [En línea]. Disponible en: https://www.kaspersky.es/resource-center/threats/viruses-worms .

CO.NORTON. ¿Qué es un troyano?, [En línea]. Disponible en: https://co.norton.com/internetsecurity-malware-what-is-a-trojan.html .

CISET. Spyware-programa espía, [En línea]. Disponible en: https://www.ciset.es/glosario/488-spyware .

MALWAREBYTES. ¿Qué es el adware?, [En línea]. Disponible en: https://es.malwarebytes.com/adware/ .

PANDASECURITY. ¿Qué es un ransomware?, [En línea]. Disponible en: https://www.pandasecurity.com/spain/mediacenter/malware/que-es-un-ransomware/ .

SEGU-INFO. Phishing, [En línea]. Disponible en: https://www.segu-info.com.ar/malware/phishing.htm .

CAPACITY. Las 8 mejores herramientas de seguridad y hacking, [En línea]. Disponible en http://blog.capacityacademy.com/2012/07/11/las-8-mejores-herramientas-de-seguridad-y-hacking/

GITHUB. Características SQLMap, [En línea]. Disponible en: https://github.com/sqlmapproject/sqlmap/wiki/Features

MSNSEGURIDAD. Anatomía de un Ataque Informático, [En línea]. Disponible en: http://msnseguridad.blogspot.com/2012/08/anatomia-de-un-ataque-informatico.html.

SYSADM. Actualizar PostgreSQL Versiones, [En linea]. Disponible en: https://sysadm.es/actualizar-postgresql-versiones-major/

TODOPOSTGRESQL. Actualización de PostgreSQL, [En línea]. Disponible en: https://todopostgresql.com/actualizacion-de-postgresql/

LOPEZ Henry, PAREDES Oscar. Mitigación de Ataques DDoS en Base de Datos Mediante un Balanceador de Carga. [En línea]. Disponible en: https://journal.espe.edu.ec/ojs/index.php/geeks/article/download/278/257 .

BLOG.SUCURI. ¿Qué es un WAF? [En línea]. Disponible en: https://blog.sucuri.net/espanol/2018/01/que-es-un-waf.html.

SECURIZANDO. WAF-Web Application Firewall. [En línea]. Disponible en: https://securizando.com/waf-web-application-firewall/.

GUADALUPE JOSÉ. Identificación y Clasificación de las Mejores Prácticas para Evitar la Inyección SQL. [En línea]. Disponible en: https://cimat.repositorioinstitucional.mx/jspui/bitstream/1008/412/1/ZACTE16.pdf.

UNAB. Database Main Threats Analisys, [En línea]. Disponible en: http://www.unab.edu.co/sites/default/files/MemoriasGrabadas/papers/capitulo9_paper_10.pdf.

OWASP. Estándar de verificación de seguridad en aplicaciones, [En línea]. Disponible en: https://www.owasp.org/images/6/67/OWASPApplicationSecurityVerificationStandard3.0.pdf.

TIPTON Harold, KRAUSE Micki. Information security management handbook, 5th. 2006

GÓMEZ Iván, Diseño de metodología para verificar la seguridad en aplicaciones web contra inyecciones SQL, [En línea]. Disponible en: https://repository.unimilitar.edu.co/bitstream/handle/10654/7212/GomezGonzalezIvanCamilo2012.pdf?sequence=2&isAllowed=y

POSTGRESQL. E.3 Versión 12, [En línea]. Disponible en: https://www.postgresql.org/docs/12/release-12.html

UBUNLOG. Liberadas las nuevas versiones de PostgreSQL 11 [En línea]. Disponible en: https://ubunlog.com/liberadas-las-nuevas-versiones-de-postgresql-11-3-y-10-8-con-mas-de-60-errores-solucionados/.

POSTGRESQL. Comunicado de prensa para Postgres 10 [En línea]. Disponible en: https://www.postgresql.org/about/press/presskit10/es/

POSTGRESQL. E.9 Versión 9.6 [En línea]. Disponible en: https://www.postgresql.org/docs/9.6/release-9-6-9.html

POSTGRESQL. E.9 Versión 9.5 [En línea] Disponible en: https://www.postgresql.org/docs/9.5/release-9-5-13.html

POSTGRESQL. E.9 Versión 9.4 [En línea]. Disponible en: https://www.postgresql.org/docs/9.4/release-9-4-18.html

POSTGRESQL. E.9 Versión 9.3 [En línea]. Disponible en: https://www.postgresql.org/docs/9.3/release-9-3-23.html

DAIGOR. Instalación y Configuración Inicial de PostgreSQL-11, [En línea]. Disponible en https://daigor.dev/post/postgres11-conf-init/

RESUMEN ANALÍTICO ESPECIALIZADO
RAE

Tema	**VULNERABILIDADES EN LAS BASES DE DATOS POSTGRESQL**
Título	MITIGAR LOS RIESGOS DE ATAQUES A BASES DE DATOS POSTGRESQL, DE LA FAMILIA DE LAS VERSIONES 9.X, EN AMBIENTES WEB.
Nombres y Apellidos del Autor	**José Alain Salazar Cataño**

Fuente Bibliográfica

SECURELIST. Desarrollo de las amenazas informáticas en el primer trimestre de 2018, [En línea]. Disponible en https://securelist.lat/it-threat-evolution-q1-2018-statistics/86929/

VILLALOBOS Johnny. Vulnerabilidades de Sistemas Gestores de Base de Datos, [En línea]. Disponible en: https://www.redalyc.org/html/4759/475948929016/

AMERICA-RETAIL. Colombia: el comercio electrónico y su potencial en el pais, [En línea]. Disponible en: https://www.america-retail.com/colombia/colombia-el-comercio-electronico-y-su-potencial-en-el-pais/

CVE-2015-3165. Vulnerabilidad 2015-3165, [En línea]. Disponible en: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3165 .

BLOG.UTP. Seguridad y protección de los sistemas operativos, [En línea]. Disponible en: http://blog.utp.edu.co/seguridadso/ .

CERTSUPERIOR S DE RL DE CV. Seguridad en redes, [En línea]. Disponible en: https://www.certsuperior.com/SeguridadenRedes.aspx .

CLAVADETSCHER Charles. Autorización en PostgreSQL, 2015. [En línea]. Disponible en: http://www.schmiedewerkstatt.ch/documents/04-publications/autorizacion_en_postgresql_script_pdfa.pdf .

EMC2NET. PostgreSQL y el uso de SSL, [En línea]. Disponible en: https://e-mc2.net/es/postgresql-y-el-uso-de-ssl .

TENER Simón, PEQUEÑO Nelson. Respaldo y recuperación de datos. 2000, [En línea]. Disponible en: https://es.slideshare.net/asaelito/respaldo-y-recuperacion-de-informacion .

2NDQUADRANT. Actualizar PostgreSQL, [En línea]. Disponible en: https://www.2ndquadrant.com/es/servicios/actualizar-postgresql/ .

EL CONGRESO DE COLOMBIA. Ley 1273 de 2009, [En línea]. Disponible en: http://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf .

UNISDR.ORG. ¿Qué significa vulnerabilidad?, [En línea]. Disponible en: https://www.unisdr.org/2004/campaign/booklet-spa/page8-spa.pdf.

PLATZI. ¿Qué es PostgreSQL y cuáles son sus ventajas?, [En línea]. Disponible en: https://platzi.com/blog/que-es-postgresql/ .

EPN. Riesgo, Amenaza y Vulnerabilidad, [En línea]. Disponible en: http://epn.gov.co/elearning/distinguidos/SEGURIDAD/13_riesgo_amenaza_y_vulnerabilidad.html

Universidad Nacional de Luján. Amenazas a la seguridad de la información, [En línea]. Disponible en: http://www.seguridadinformatica.unlu.edu.ar/?q=node/12 .

ECURED. Bases de Datos, [En línea]. Dsiponible en: https://www.ecured.cu/Bases_de_datos .

SEARCHDATACENTER. Networking, redes, cableado.. similitudes y diferencias, [En línea]. Disponible en: https://searchdatacenter.techtarget.com/es/consejo/Networking-redes-cableado-similitudes-y-diferencias .

TECNOLOGÍA-INFORMÁTICA. ¿Qué es un router?, [En línea]. Disponible en: https://tecnologia-informatica.com/que-es-router-wifi-comprar-ampliar-alcance/ .

LATAM-KASPERSKY. ¿Qué es un firewall?, [En línea]. Disponible en: https://latam.kaspersky.com/resource-center/definitions/firewall .

SOFTWAREDOIT. Definición términos de software, [En línea]. Disponible en: https://www.softwaredoit.es/definicion/index.html .

VIX. ¿Qué es un hacker?, [En línea]. Disponible en: https://www.vix.com/es/btg/tech/13182/que-es-un-hacker .

CONSULTHINK.IT. ¿Qué es y en qué consiste un ataque informático?, [En línea]. Disponible en: https://consulthink.it/es/que-es-y-en-que-consiste-un-ataque-informatico/ .

ONA SYSTEMS. Vulnerabilidades importantes que afectan la seguridad de bases de datos en las empresas, [En línea]. Disponible en: https://www.onasystems.net/vulnerabilidades-importantes-afectan-la-seguridad-bases-datos-las-empresas/ .

AVAST. Malware & Antimalwalre, [En línea]. Disponible en: https://www.avast.com/es-es/c-malware .

INFOSPYWARE. ¿Qué son los virus informáticos?, [En línea]. Disponible en: https://www.infospyware.com/articulos/%C2%BFque-son-los-virus-informaticos/ .

KASPERSKY. Gusanos informáticos, [En línea]. Disponible en: https://www.kaspersky.es/resource-center/threats/viruses-worms .

CO.NORTON. ¿Qué es un troyano?, [En línea]. Disponible en: https://co.norton.com/internetsecurity-malware-what-is-a-trojan.html .

CISET. Spyware-programa espía, [En línea]. Disponible en: https://www.ciset.es/glosario/488-spyware .

MALWAREBYTES. ¿Qué es el adware?, [En línea]. Disponible en: https://es.malwarebytes.com/adware/ .

PANDASECURITY. ¿Qué es un ransomware?, [En línea]. Disponible en: https://www.pandasecurity.com/spain/mediacenter/malware/que-es-un-ransomware/ .

SEGU-INFO. Phishing, [En línea]. Disponible en: https://www.segu-info.com.ar/malware/phishing.htm .

CAPACITY. Las 8 mejores herramientas de seguridad y hacking, [En línea]. Disponible en http://blog.capacityacademy.com/2012/07/11/las-8-mejores-herramientas-de-seguridad-y-hacking/

GITHUB. Características SQLMap, [En línea]. Disponible en: https://github.com/sqlmapproject/sqlmap/wiki/Features

MSNSEGURIDAD. Anatomía de un Ataque Informático, [En línea]. Disponible en: http://msnseguridad.blogspot.com/2012/08/anatomia-de-un-ataque-informatico.html.

SYSADM. Actualizar PostgreSQL Versiones, [En linea]. Disponible en: https://sysadm.es/actualizar-postgresql-versiones-major/

TODOPOSTGRESQL. Actualización de PostgreSQL, [En línea]. Disponible en: https://todopostgresql.com/actualizacion-de-postgresql/

LOPEZ Henry, PAREDES Oscar. Mitigación de Ataques DDoS en Base de Datos Mediante un Balanceador de Carga. [En línea]. Disponible en: https://journal.espe.edu.ec/ojs/index.php/geeks/article/download/278/257 .

BLOG.SUCURI. ¿Qué es un WAF? [En línea]. Disponible en:

https://blog.sucuri.net/espanol/2018/01/que-es-un-waf.html.
SECURIZANDO. WAF-Web Application Firewall. [En línea]. Disponible en: https://securizando.com/waf-web-application-firewall/.

GUADALUPE JOSÉ. Identificación y Clasificación de las Mejores Prácticas para Evitar la Inyección SQL. [En línea]. Disponible en: https://cimat.repositorioinstitucional.mx/jspui/bitstream/1008/412/1/ZACTE16.pdf.

UNAB. Database Main Threats Analisys, [En línea]. Disponible en: http://www.unab.edu.co/sites/default/files/MemoriasGrabadas/papers/capitulo9_paper_10.pdf.

OWASP. Estándar de verificación de seguridad en aplicaciones, [En línea]. Disponible en: https://www.owasp.org/images/6/67/OWASPApplicationSecurityVerificationStandard3.0.pdf.

TIPTON Harold, KRAUSE Micki. Information security management handbook, 5th. 2006

GÓMEZ Iván, Diseño de metodología para verificar la seguridad en aplicaciones web contra inyecciones SQL, [En línea]. Disponible en: https://repository.unimilitar.edu.co/bitstream/handle/10654/7212/GomezGonzalezIvanCamilo2012.pdf?sequence=2&isAllowed=y

POSTGRESQL. E.3 Versión 12, [En línea]. Disponible en: https://www.postgresql.org/docs/12/release-12.html

UBUNLOG. Liberadas las nuevas versiones de PostgreSQL 11 [En línea]. Disponible en: https://ubunlog.com/liberadas-las-nuevas-versiones-de-postgresql-11-3-y-10-8-con-mas-de-60-errores-solucionados/.

POSTGRESQL. Comunicado de prensa para Postgres 10 [En línea]. Disponible en: https://www.postgresql.org/about/press/presskit10/es/

POSTGRESQL. E.9 Versión 9.6 [En línea]. Disponible en: https://www.postgresql.org/docs/9.6/release-9-6-9.html

POSTGRESQL. E.9 Versión 9.5 [En línea] Disponible en: https://www.postgresql.org/docs/9.5/release-9-5-13.html

POSTGRESQL. E.9 Versión 9.4 [En línea]. Disponible en: https://www.postgresql.org/docs/9.4/release-9-4-18.html

POSTGRESQL. E.9 Versión 9.3 [En línea]. Disponible en: https://www.postgresql.org/docs/9.3/release-9-3-23.html
DAIGOR. Instalación y Configuración Inicial de PostgreSQL-11, [En línea].

Disponible en https://daigor.dev/post/postgres11-conf-init/

Año	**2020**

Resumen:
Postgresql pertenece a la categoría de base de datos relacionales, por esta razón es una de las opciones más interesantes, al momento de pensar en alojar y administrar la información, es utilizada para entornos cliente servidor y aplicaciones web, debido a que permite desarrollar bases de datos relacionales robustas y eficientes, sin embargo, es susceptible de ser atacada, debido a múltiples causas que generan fallas de seguridad tanto internas como externas, por esta razón es preciso referenciar que históricamente los expertos en seguridad de postgresql, han encontrado de cero a siete problemas de seguridad al año, a esto debemos añadirle que en Colombia se registran al día 542 mil ataques informáticos, donde el sector financiero es el blanco principal de estos ataques y que solo el 37% de las empresas, manifiesta estar preparado para hacer frente a un incidente digital, de este porcentaje el 70% corresponde a grandes empresas y para el caso de las microempresas solo el 45%.

Por las razones expuestas, es necesario identificar las vulnerabilidades encontradas en este manejador de base de datos, identificando las actualizaciones que corrigen dichos fallos y proponer una metodología de aseguramiento que mitigue el riesgo de intrusión que comprometa la información almacenada para las versiones de la familia 9.x de postgresql, para lograr este objetivo, es necesario realizar un análisis, que permita identificar los requerimientos de hardware y software y el tipo de implementación de seguridad, con el que debe contar un ambiente de producción de postgresql versiones 9.x en ambientes web.

Palabras Claves	PostgreSQL, Ataques, Vulnerabilidades, Riesgos, Mitigar, Actualizaciones, PHVA

Contenidos:
Inicialmente se describen las vulnerabilidades encontradas en la base de datos, para proceder a plantear los procedimientos que se deben seguir para mitigar y evitar ataques que comprometan la información albergada en el SGBD, igualmente se consultan las actualizaciones publicadas por el fabricante, para solucionar problemas de seguridad encontrados en el SGBD y finalmente se plantea una metodología que permita mitigar las vulnerabilidades y riesgos de seguridad del SGBD PostgreSQL

Descripción del problema de investigación:
En la actualidad Postgresql sufre ataques de inyección SQL, elevación de privilegios, malware, uso excesivo de privilegios y denegación del servicio a causa del mal diseño de las aplicaciones, bases de datos mal configuradas, falta de actualizaciones tanto del sistema operativo como del sistema gestor de base de datos, redes y sistemas operativos expuestos, por falta de hardware y/o software que impida o detecte el acceso no autorizado a las redes locales y al equipo que alberga el sistema gestor de la base de datos postgresql.

Según un informe de TECNONUCLEOUS El ataque más conocido a postgresql se presentó mediante malware donde se utilizó una imagen de la actriz scarlett Johansson, que contenía una carga maliciosa para luego instalarse como un minero de monero, este ataque fue descubierto por el honeypot de la firma de seguridad imperva, revelando que más de 710,000 servidores estaban visibles en internet y eran vulnerables a este tipo de ataque.

Así mismo durante el primer trimestre de 2018 el common vulnerabilities and exposures (CVE), reveló 4 vulnerabilidades encontradas en el SGBD que permitía que un atacante autenticado leyera bytes de la memoria del servidor, leer o modificar archivos que pueden contener contraseñas de base de datos cifradas y no cifradas, escalar privilegios y ejecutar código con permiso de superusuario en la base de datos.

Objetivo general:
Determinar las vulnerabilidades existentes en las bases de datos postgresql, versiones 9x, con el fin de mitigar los riesgos y reducir la posibilidad de intrusión en un 70%.

Objetivos específicos:

- Describir las vulnerabilidades encontradas a la familia de las versiones 9.x, las cuales han sido reportadas al CVE (Common Vulnerabilities and Exposures).
- Identificar las actualizaciones que corrigen las vulnerabilidades que afectan la familia de las versiones 9.x
- Documentar los procedimientos establecidos para prevenir, ataques por fallas o vulnerabilidades del sistema de gestión de base de datos.
- Proponer una metodología de aseguramiento que mitigue el riesgo de intrusión, para la familia de versiones postgresql 9.x.

Metodología: La presente monografía, se realizó con base en la consulta y análisis de los diferentes textos referenciados en el marco teórico y conceptual, en busca de proponer un mecanismo que permita mitigar las vulnerabilidades presentes en las bases de datos postgreslq.

Principales Referentes Teóricos y Conceptuales:
MARCO TEÓRICO

- Reporte de Vulnerabilidades de PostgreSQL Familia 9.x
- Aspectos a tener en cuenta para la seguridad de la base de datos PostgreSQL
- Normatividad en Colombia, ley 1273 de 2009 “Delitos Informáticos en Colombia”
- Ley 599 de 2000, Código Penal Colombiano
- Ley Estatutaria 1266 de 2008
- Ley Estatutaria 1581 de 2012
- Decreto 2693 de 2012
- Ley 1712 de 2014

MARCO CONCEPTUAL

- Tipo de Vulnerabilidades
- Ataques Informáticos
- Herramientas para Escanear Vulnerabilidades a Base de Datos
- Anatomía de un Ataque Informático
- Actualizaciones de Seguridad en PostgreSQL
- Procedimiento para Prevenir Ataques
- Metodología para Prevenir Intrusiones a las Bases de Datos PostgreSQL

Resultados:

Para abordar el problema y dar una solución que mitigue el riesgo de intrusión a las bases de datos PostgreSQL, es necesario que dicho planteamiento se base en el ciclo de mejora continua PHVA.

Este planteamiento se debe a que la tecnología no para de avanzar, somos conscientes que día a día el poder de procesamiento aumenta, se desarrollan nuevas herramientas para proteger y atacar en la red, por tanto cualquier metodología deba plantearse como un ciclo de mejora continua.

Planeación

En esta etapa debemos considerar los siguientes elementos

- **Identificación**: En este paso se deben analizar las aplicaciones que requieren ser protegidas, estas aplicaciones comprenden el sistema gestor de base de datos, sistemas operativos y aplicaciones que se conectan a la base de datos.
- **Recopilación**: Se debe recopilar toda la documentación con que se cuenta, a cerca de la configuración del motor de base de datos, sistema operativo que aloja el motor de base de datos, diccionario, manual de desarrollo y manual del usuario de las aplicaciones que se conectan a las base de datos postgresql de la organización, adicional a esto es necesario contar con la documentación del lenguaje de programación, con el que se desarrollaron dichas aplicaciones.
- **Definir los Parámetros a Mejorar**: En este paso se debe establecer, cuáles son los parámetros que se deben mejorar, producto de la identificación y la recopilación de la documentación realizada en las etapas anteriores, igualmente se debe hacer un análisis para verificar el cumplimiento de seguridad del sistema gestor de base de datos, de acuerdo a los procedimientos establecidos para evitar o mitigar ataques por los diferentes métodos analizados en los numerales anteriores.

Hacer

En esta etapa se deben realizar los siguientes pasos:

Test de Vulnerabilidades: Para la realización de estas pruebas de vulnerabilidades, se deben utilizar herramientas que realicen un proceso automático de verificación como NMAP, SQLMAP, NESSUS, PIPPER, BSQL HACKER entre otras, las cuales las podemos encontrar en suites como OWASP y KALI Linux

Verificar
En esta etapa se debe documentar lo realizado en la etapa anterior, con el fin de comparar los resultados, con los objetivos trazados en la etapa de planeación, con el fin de detectar que mejoras hacen falta.

Actuar
Con base en la documentación anterior, realizar un análisis con el fin de determinar una de las tres posiciones que se relacionan a continuación:

- Determinar si los controles que se hicieron son satisfactorios y no es necesario realizar el ciclo nuevamente.
- Determinar si los controles que se hicieron no son satisfactorios y no se cumplieron las metas trazadas por tanto se debe realizar nuevamente el ciclo de mejora continua.

- Plantear la pregunta de cómo se podría mejorar la seguridad y documentar todo el proceso.

Conclusiones:

- Al analizar el reporte de vulnerabilidades para PostgreSQL 9.x, se concluye que esta versión presentaba profundas fallas de seguridad que le permitían a un intruso, realizar ataques SQL Injecction, obtener privilegios y provocar denegación de servicio.

- El fabricante PostgreSQL realizó el lanzamiento de 7 versiones menores de la familia 9x comprendidas por la 9.0.23, 9.1.24, 9.2.24, 9.3.25, 9.4.26, 9.5.21 y 9.6.17, esta última fue el fin de las versiones 9.x ya que a partir de la 10, se cambió el esquema a un formato “xy”, que significa que la siguiente versión menor sería 10.1 y la próxima principal sería la 11.

- Aproximadamente el 80% de los ataques que se presentan en las organizaciones, corresponde al uso excesivo de privilegios, convirtiéndose este, en el mayor peligro que debe afrontar y mitigar el profesional de la seguridad informática, para salvaguardar la información.

- La tarea de prevenir intrusiones a la base de datos, es un entorno cambiante e impredecible donde la mitigación, debe estar diseñada bajo el ciclo PHVA, el cual es un sistema que le permite al profesional de la seguridad informática, aplicar los procedimientos planteados y realizar la auditoria del mismo que le permite la mejora continua de la seguridad de la información.

Nombre y apellidos de quien elaboró este RAE	**José Alain Salazar Cataño**
Fecha en que se elaboró este RAE	26 de Septiembre de 2020